Unit I (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 90 minutes
UNIT TITLE	Introduction and Course Overview
OBJECTIVES	1. Describe the goal, objectives, and agenda for the course 2. Describe and find material in the course reference manual and student activity handout
SCOPE	The following topics will be covered in this unit: 1. Welcome and Opening Remarks 2. Instructor Introductions 3. Administrative Information 4. Student Introductions 5. Course Overview 6. Course Materials 7. Activity: Refamiliarize with Case Study materials
REFERENCES	1. Course Agenda 2. Course Goal and Objectives 3. Evaluation Forms (EMI or other as appropriate) 4. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* 5. Case Study – Appendix C: COOP, Cooperville Information / Business Center 6. Student Manual, Unit I (C) (info only – not in SM) 7. Unit I (C) visuals (info only – not in SM) 8. Class Roster before course start and updated at end of course (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 I (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit I (C) visuals
7. Risk Matrix poster and one box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** This instruction unit has no linkages to the Local Area. The unit is a course overview and refamiliarization with the contents of the COOP Case Study.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will begin refamiliarizing themselves with the Case Study materials. The Case Study is a risk assessment and analysis of mitigation options and strategies for a typical commercial office building located in a mixed urban-suburban environment business park that is being evaluated as a Continuity of Operations alternate facility. The assessment will use the DoD Antiterrorism Standards and the GSA Interagency Security Criteria to determine Levels of Protection and identify specific vulnerabilities, as well as Federal Preparedness Circular-65 for COOP specific requirements. Mitigation options and strategies will use the concepts provided in **FEMA 426** and other reference materials.

- Refer students to their Student Manual 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. Note that this Student Activity provides page numbers for each question to assist the students in their familiarization and answering of the questions.

- 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. This latter point may not be evident in this first student activity.

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

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

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

- Ask for and answer questions.

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

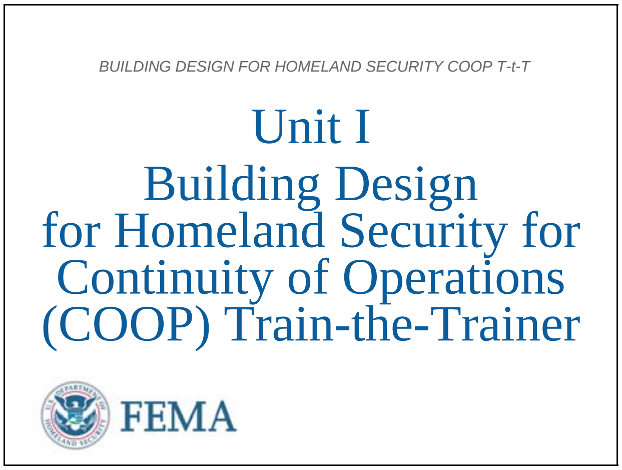
(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-1



Welcome and Opening Remarks

Welcome the students to the Building Design for Homeland Security Course.

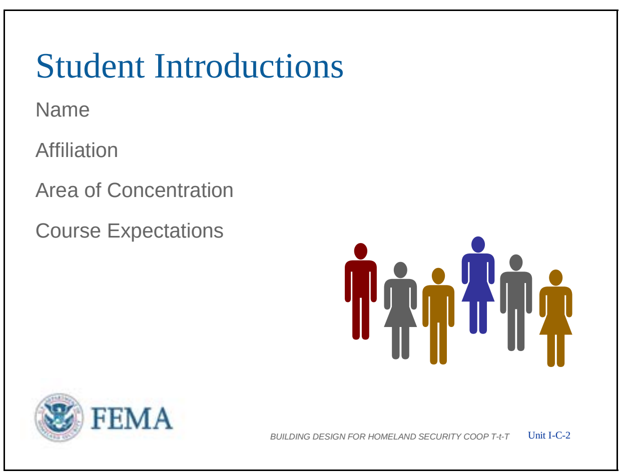
Introduce yourself and have the other instructors introduce themselves, using:

- Your name
- Your company or organization
- Brief statement of background and experience

Make the necessary administrative announcements, including:

- Housing, parking, and meals
- Attendance, start/stop times, breaks
- Restroom locations
- Messages and emergencies
- Fire exits

VISUAL I-C-2



Recommend an instructor not presenting Unit I to collect Student Expectations on an easel tablet for reference throughout the course and review in Unit XIV.

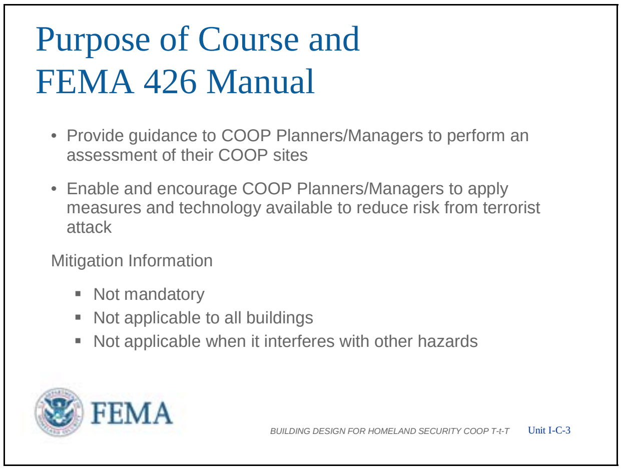
Student Introductions

Ask the students to introduce themselves, including:

- Name
- Affiliation
  - o Brief statement of background and experience
  - o Include any work done in course topic area
- Reasons they are attending course / course expectations. [These will be reviewed during Unit XIV, Course Wrap-Up.]

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-3



Purpose

The purpose of **FEMA 426** and this course is to provide guidance to the building sciences community working for public and private institutions. It presents tools to help decision-makers assess the performance of their buildings against terrorist threats and to rank recommendations. It is up to the decision-makers to decide which types of threats they wish to protect against and to determine their level of risk against each threat. Those decision-makers who consider their buildings to be at high risk can use this guidance as necessary.

The mitigation information in **FEMA 426** and this course is:

- Not mandatory
- Not applicable to all buildings
- Not applicable when it interferes with other hazards such as fire, seismic, or life safety requirements contained in building codes

VISUAL I-C-4

Course Goals

The goals of this course are:

To enhance student understanding of the measures and technology available to reduce risk from terrorist attack.

To enhance student ability to assess a site for COOP requirements and natural and man-made hazards

Included in this understanding is the process for assessing risk to focus upon which mitigation measures have the greatest applicability and benefit. The students will understand the design approaches to mitigate manmade hazards and comprehend the trade-

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

offs needed to optimize various design requirements.

VISUAL I-C-5

Course Objectives

Students will be able to:

1. **Explain** the basic components of the assessment methodology.
2. **Appreciate** the different assessment methodology approaches that can be used.
3. **Perform** an assessment for a building by identifying and prioritizing assets, threats, and vulnerabilities and calculating relative risk.

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit I-C-5

Course Objectives (1 of 3)

The primary target audience for this course version is COOP planners, COOP managers, COOP engineers, and COOP assessors. The basic course from which this course is derived has a target audience of engineers, architects, and state and local government and building officials with engineering and architectural backgrounds involved in mitigation planning and design to protect people and property against manmade hazards. Security personnel and first responders have also attended to understand the concerns of man-made hazards and the impact upon their areas of responsibility.

After attending the Building Design for Homeland Security course, the students should be able to:

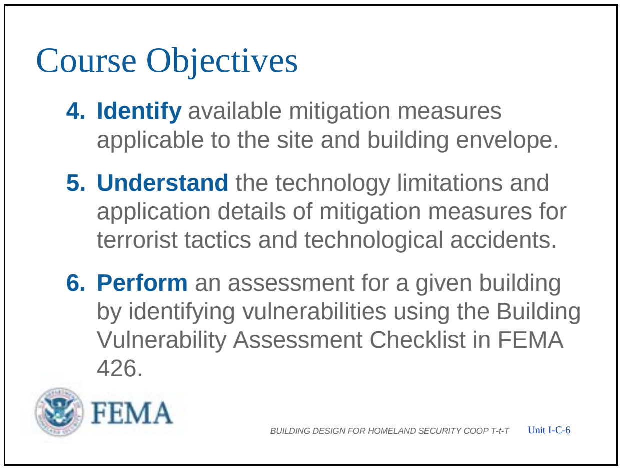
1. Explain the basic components of the assessment methodology – threat/hazard, asset value, vulnerability, and risk, as applied to site, layout, and building.

2. Appreciate the different assessment methodology approaches being used by Federal agencies and comprehend which approach to use for a given organizational structure.

3. Perform an assessment for a given building by identifying the assessment components and prioritizing the asset-threat/hazard pairs by their relative risk to focus resources upon mitigation measures that reduce risk.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-6



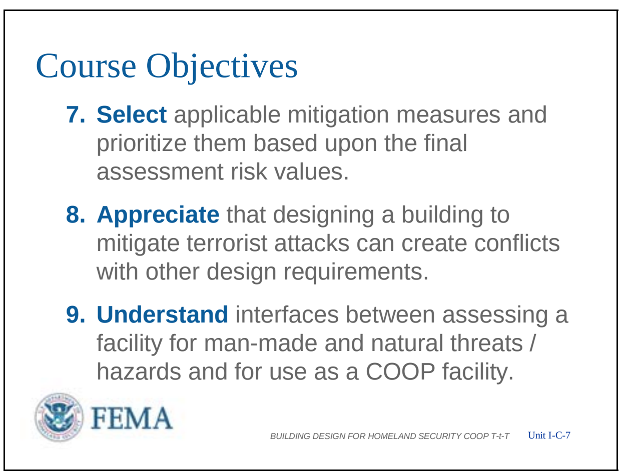
Course Objectives (2 of 3)

4. Identify available mitigation measures either in-place or for new design and comprehend their applicability to a given situation.

5. Understand the technology limitations and application details of mitigation measures for terrorist tactics and technological accidents involving explosive blast and agent release (chemical, biological, and radiological) to achieve a desired level of protection.

6. Use the **Building Vulnerability Assessment Checklist in FEMA 426 (Table 1-22, pages 1-46 to 1-93)** and adjust the assessment relative risk based upon the identified vulnerabilities.

VISUAL I-C-7



Course Objectives (3 of 3)

7. Select applicable mitigation measures and prioritize them based upon the final assessment relative risk values and associated estimated risk reduction provided so as to focus limited resources, all for a given situation.

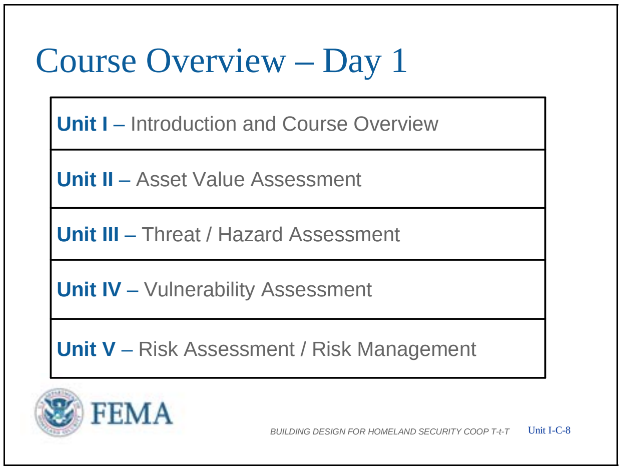
8. Appreciate that designing to mitigate building vulnerabilities against terrorist attacks has conflicts with other design requirements, resulting in trade-offs to achieve acceptable compliance and levels of performance among the differing regulations, codes, programs, operational requirements, and owner desires within the resources available.

9. Understand that, as with balancing mitigation trade-offs with other design requirements, the interfaces (duplicate concerns versus separate specific

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

assessment concerns) among assessing a facility for man-made threats/hazards, for natural threats/hazards, and for use as a COOP facility.

VISUAL I-C-8



Course Overview – Day 1

This course is a full 3 days in length and includes 14 units of instruction. Most instruction blocks have an associated student activity using a Case Study to emphasize the concepts taught and apply what was just learned.

A detailed schedule is located in your Student Manuals. This is Unit I – Introduction and Course Overview. It will review the other blocks of instruction and the course materials.

For the rest of the first day, the course will introduce the components of risk and how to determine risk. Unit II – Asset Value Assessment will discuss how to identify assets – or things to be protected, and how to assign a relative value to them.

Unit III will examine the Threat/Hazard Assessment process and identify the threats and hazards that could impact a building or site, describe how to assess these threats and hazards, and provide a numerical rating for the threat or hazard.

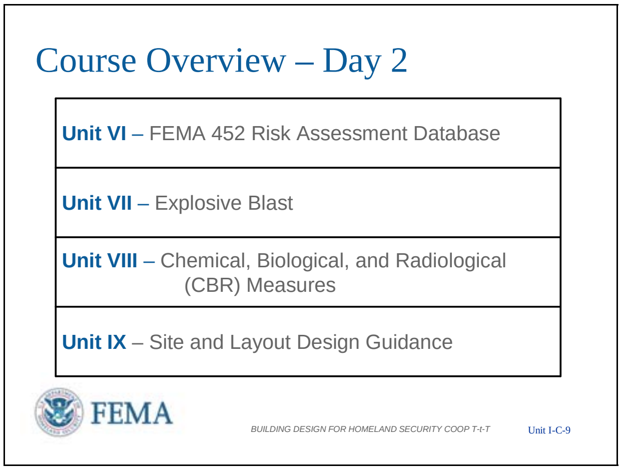
Unit IV will cover Vulnerability Assessment, including what constitutes vulnerability and how to identify vulnerabilities using the **Building Vulnerability Assessment Checklist in FEMA 426 (Table 1-22, pages 1-46 to 1-93).**

Finally, the last Topic that will be covered on Day 1 is Unit V – Risk Assessment / Risk Management. Students will be taught what constitutes risk and how to determine a

INSTRUCTOR NOTES	CONTENT/ACTIVITY

numerical value for risk and be introduced to the concept of the Design Basis Threat. This unit will be completed on Day 2.

VISUAL I-C-9



Course Overview – Day 2

Day 2 will start with Unit VI which presents the associated software database. The database is an electronic way of managing the information you collected manually yesterday to assess risk, make observations, and identify vulnerabilities and mitigation measures, track actions, and generate reports. The database presents an efficient way to manage the diverse information collected during a risk and vulnerability assessment.
[Options: If you brought a laptop, you can use the FEMA 452 Database CD to follow along the presentation, by installing and navigating the database. However, the demonstration / performance approach has not been fully successful for various reasons, so opportunity at lunch and at the end of the day will be made to assist in loading the database.]

Units VII and VIII will provide students with an understanding of some of the weapons commonly used by terrorists. Unit VII will cover explosive blast and Unit VIII will cover chemical, biological, and radiological or CBR weapons.

Unit IX – Site and Layout Design Guidance will cover things you can do to mitigate terrorist attacks for the site – meaning from the property line up to the building.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL I-C-10

Course Overview – Day 3

Unit X – Building Design Guidance (continued)	
Unit XI – Electronic Security Systems	
Unit XII – Finalization of Case Study Results	
Unit XIII – Train-the-Trainer	
Unit XIV – Course Wrap-up	

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit I-C-10

Course Overview – Day 3

Unit X will explore mitigation options for the building envelope and inside the building.

Unit XI will introduce the basic concepts of electronic security systems.

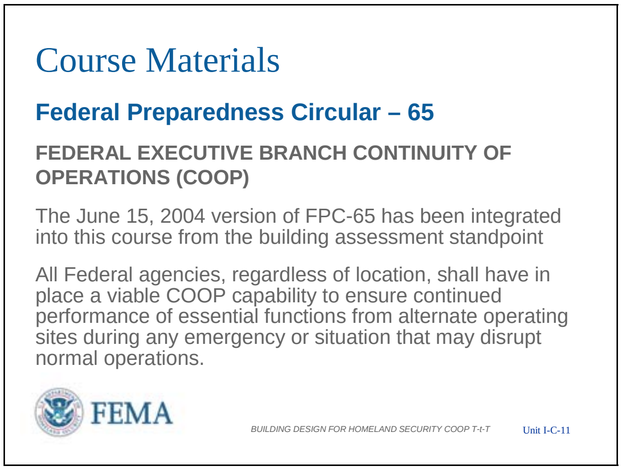
As mentioned earlier – each block of instruction has an associated student activity using a Case Study to emphasize the concepts taught and apply what was just learned. In Unit XII, students will present the results of their work using the Case Study – highlighting their top three risks identified by the group, the vulnerabilities identified for these risks, and the top three mitigation measures to reduce vulnerability and risk. One member of the group will have about 5 minutes to brief their team's results. [This is the second component of the grading system for resident courses at the Emergency Management Institute.]

Unit XIII – Train-the-Trainer will clarify the procedures used to set up and deliver the course and answer any student questions about preparation and delivery.

Finally, Unit XIV will summarize the key points from the course and answer any final questions.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

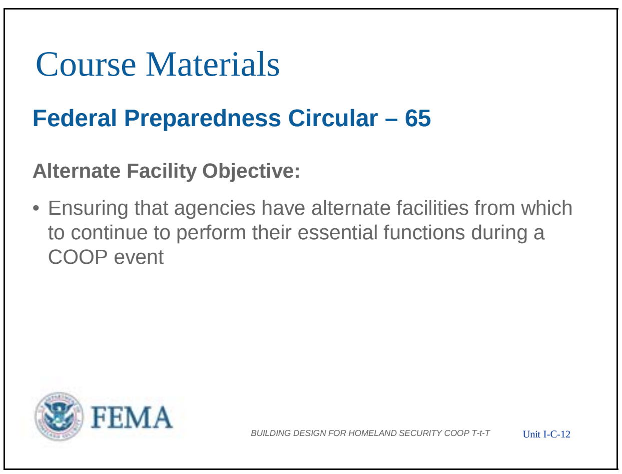
VISUAL I-C-11



FPC-65

This publication's requirements are integrated into this course to supplement the building assessment, since this course deals with assessing an Alternate COOP facility.

VISUAL I-C-12

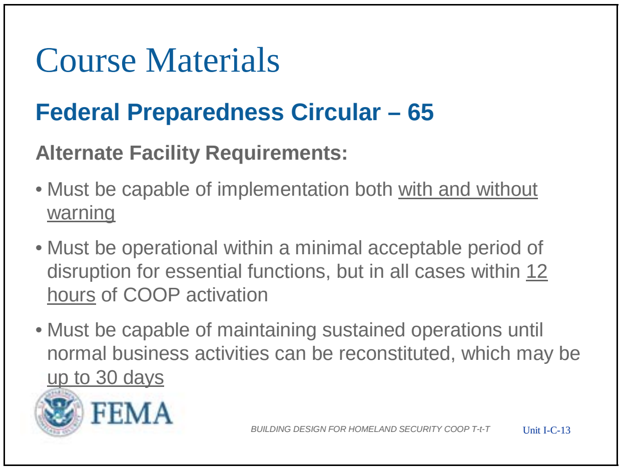


FPC-65 – Alternate Facility Objective

Each Federal agency needs alternate facilities to ensure continuation of essential functions.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-13

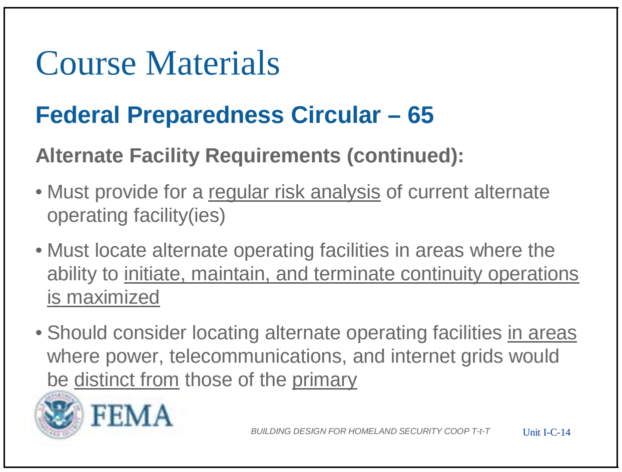


FPC-65 – Alternate Facility Requirements (1 of 3)

- Activate with or without warning
- Operational within a max of 12 hours
- Can operate for up to 30 days

NOTE: The above underlined shows on projected slide but not on thumbnail to left.

VISUAL I-C-14



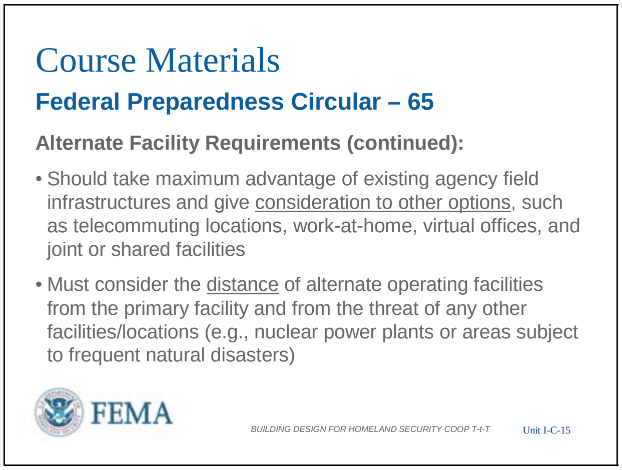
FPC-65 – Alternate Facility Requirements (2 of 3)

- Perform a regular risk analysis (one of the reasons for this course)
- Maximize continuity operations to initiate, maintain and terminate [initiate, maintain, and terminate continuity operations]
- Ensure utilities serving primary facility are not the same serving the alternate facility (so that a single event does not affect both facilities simultaneously, degrading the ability of the alternate facility to support Continuity of Operations) [in areas. ..distinct from ...primary]

NOTE: Ditto underlined above shows on projected slide but not on thumbnail to left.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL I-C-15



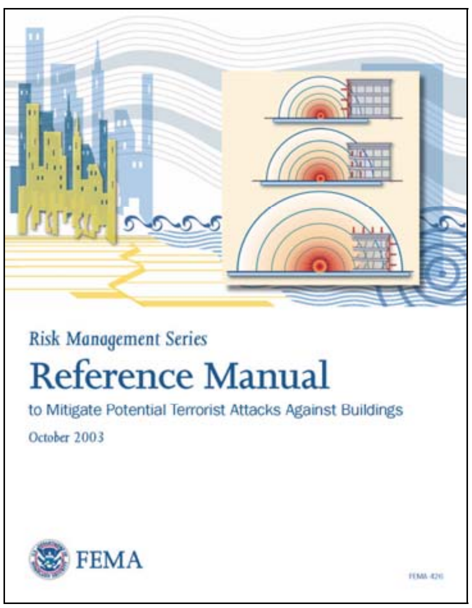
FPC-65 – Alternate Facility Requirements (3 of 3)

- Considerations of other options to alternate COOP facilities (not part of this course)

- Distance between primary facility and alternate COOP facility ensures collateral damage from technological hazards or natural disasters do not affect both sites.

NOTE: Ditto underlined above shows on projected slide but not on thumbnail to left.

NO SLIDE – USE HARDCOPY



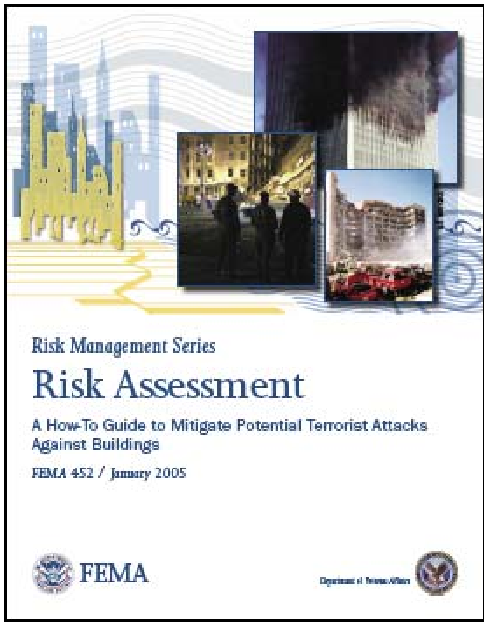
Display a copy of **FEMA 426**

FEMA 426

- This is the primary reference for this course
- Throughout the course, slides will contain references to figure and page number, as appropriate, in this document.
- There will be a comprehensive introduction to the document later in this unit.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

NO SLIDE – USE HARDCOPY

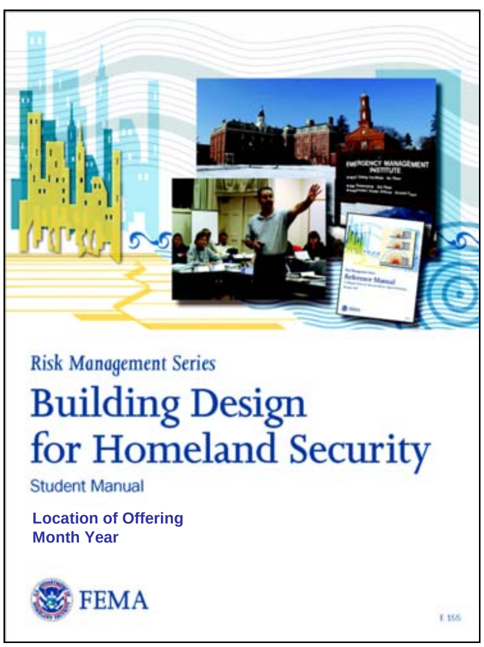


Display a copy of **FEMA 452.**

FEMA 452

- This is the "How-To" document that supplements FEMA 426 and expands the content of instruction units 2, 3, 4, and 5.
- It introduces the FEMA 452 Databases as the Risk Management tools to support the assessment and mitigation processes
- Similar to FEMA 426, the slides will contain reference to figure and page number taken from this document, as appropriate, as well as other publications

NO SLIDE – USE HARDCOPY



Display a copy of the **Student Manual** binder.

Student Manual

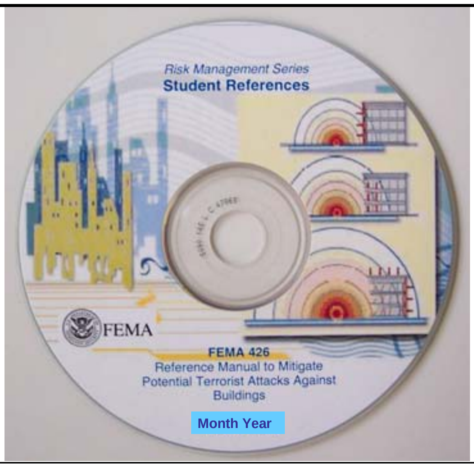
- The Student Manual will be primarily used as a workbook for activities designed to apply major teaching points.

- Each unit contains worksheets that will be completed in the small group student activity sections of each unit.

- **Appendix C** of the Student Manual is the COOP Case Study: Cooperville Information / Business Center (CI/BC) that you were asked to read prior to beginning this course.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

NO SLIDE – USE HARDCOPY



Show the double-sided media storage package containing the **Student Reference CD** and the **FEMA 452 Databases CD**.

Student References CD

- The Student Reference CD contains electronic copies of various documents that will be referenced during this course and many that are contained in the Bibliography contained in FEMA 426.
- Tell students that they should have this CD in their handout packages at their seats.

NO SLIDE – USE HARDCOPY

Show the reverse side of the media storage package to show the **FEMA 452 Databases CD**.

FEMA 452 Databases CD

[Depending upon presentation option used, the database may already have been downloaded from the FEMA web site and installed by the students on their computers – See IG Unit 6 (C) for guidance.]

- The FEMA 452 Databases CD contains the installation programs, User Guides, and files that will be used to demonstrate the features, capabilities, and operation of the databases.
- Tell students that they should have this CD in their handout packages at their seats.
- Point out to the students that the CD found inside the back cover of FEMA 452 is the enterprise version (Version 1.0) of the database as explained in the appendices at the end of that publication. The CD handed out is the COOP version (Version 3.0) of the database. See the User Guide on this CD for installation and use instructions.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Finally, tell the students that if they would like to have help loading the database on their laptop (if they brought one) to bring the laptop on Day 2 and we will assist in loading during lunch or at the end of the day.

NO SLIDE – USE HARDCOPY

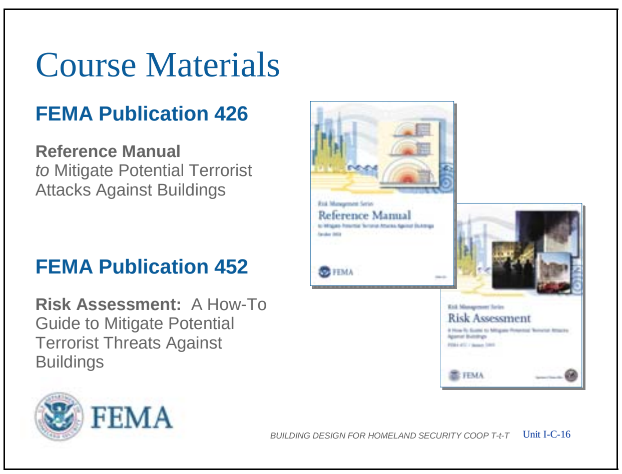
Risk Matrix Poster

Walk to a table and indicate the Risk Matrix poster (laminated with threats/hazards, critical functions, and critical infrastructure cells that the student will fill out with ratings for asset value, threat/hazard rating, vulnerability rating, and risk rating.

Risk Matrix Poster

- The small group student activities are focused on the CI/BC Case Study (COOP).
- In small groups, you will conduct a phased assessment of the CI/BC building after each step of the assessment process is introduced by the instructors.
- The final activity involves the development of possible mitigation actions to address identified risks.
- The Risk Matrix poster is provided for groups to keep a comprehensive record of their findings and for use in presenting these findings to the class.

VISUAL I-C-16



Confirm that each student has a copy of these materials.

Course Materials

At this point each student should have the following:

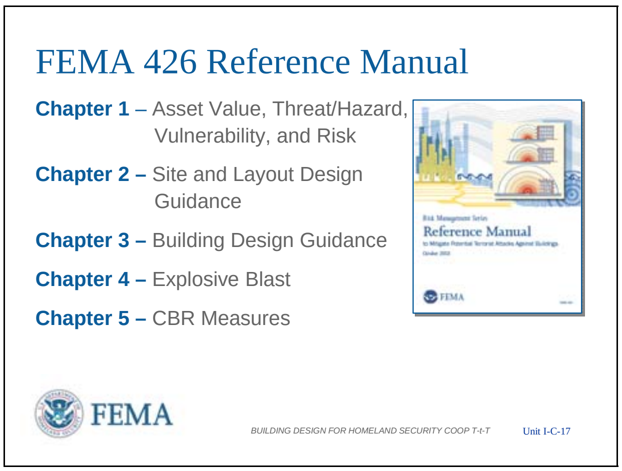
- **FEMA Publication 426**
- **FEMA Publication 452**
- Student Manual for the Case Study Version **(C - COOP)** being used in this offering of the course.
- Risk Matrix Poster
- Multi-color dry-erase markers for use on the Risk Matrix Poster.
    - o NOTE: The dry-erase markers are easy

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

to erase, meaning that anything placed on top of the posters will erase the entries – so do not place anything on the posters once you start filling them in.

Now that we have confirmed the Course Materials you should have in your possession, we will **look further into the FEMA 426 and 452 publications**.

VISUAL I-C-17



As you begin the following walk-through of **FEMA 426**:

Point out that the students will be following **FEMA 426** throughout the course and will use some sections heavily during exercises. The course visuals include **FEMA 426, FEMA 452, and other page references** for easy reference.

Encourage them to flag key pages and passages with the Post-It® notes and highlighting.

Ask them to open **FEMA 426** and follow along as you preview the contents.

FEMA 426 Reference Manual

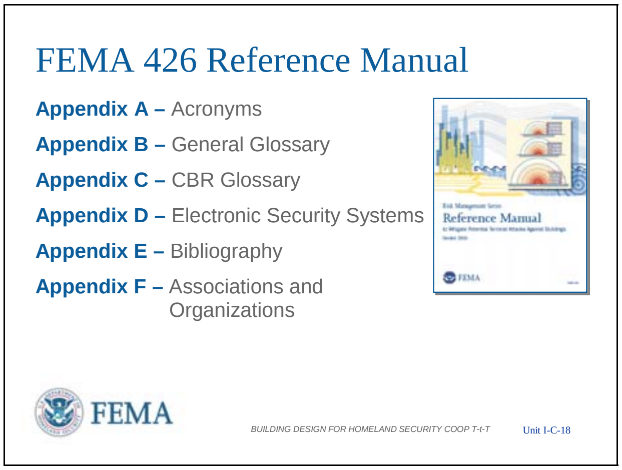
There are five chapters in the manual as listed here. This manual contains many how-to aspects based upon current information contained in FEMA, Department of Commerce, Department of Defense (including Army, Navy, and Air Force), Department of Justice, General Services Administration, Department of Veterans Affairs, Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health, and other publications. It is intended to provide an understanding of the current methodologies for assessing asset value threat/hazard, vulnerability, and risk, and the design considerations needed to improve protection of new and existing buildings and the people occupying them. As needed, this manual should be supplemented with more extensive technical resources, as well as the use of experts when necessary.

Key concepts:

- Design Basis Threat
- Levels of Protection
- Layers of Defense

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-18

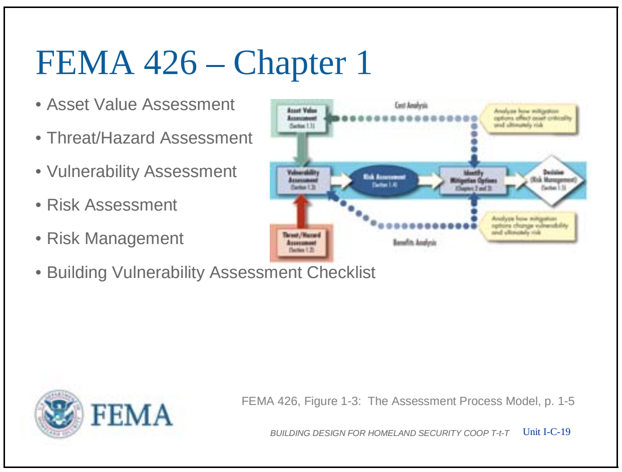


FEMA 426 Appendices

The manual also has six appendices to facilitate its use as a reference:

- Appendix A – Acronyms
- Appendix B – General Glossary
- Appendix C – CBR Glossary
- Appendix D – Electronic Security Systems
- Appendix E – Bibliography
- Appendix F – Associations and Organizations

VISUAL I-C-19



For each of the following chapters, have the students flip through each chapter and highlight some of the key concepts, graphics, etc.

FEMA 426 - Chapter 1: Asset Value, Threat/ Hazard, Vulnerability, and Risk

Chapter 1 presents selected methodologies to integrate threat/hazard, asset criticality, and vulnerability assessment information using applications such as the FEMA HAZUS-MH Geographic Information System (GIS) application to overlay imagery and maps to show access points, blast stand-off, and other site and building information.

The chapter also presents a risk matrix for the preparation of risk assessments. The topic areas of Chapter 1 are:

- Asset Value Assessment
- Threat/Hazard Assessment
- Vulnerability Assessment
- Risk Assessment
- Risk Management
- Building Vulnerability Assessment Checklist

Finally, Chapter 1 provides an assessment checklist that compiles many best practices (based upon current technologies and scientific research) to consider during the

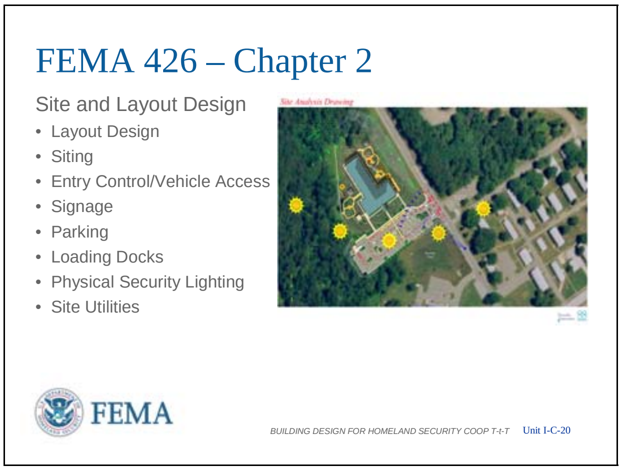
INSTRUCTOR NOTES	CONTENT/ACTIVITY

design of a new building or renovation of an existing building.

Assessment Flow Chart

The assessment flow chart illustrates the process you will follow in conducting the assessment.

VISUAL I-20



FEMA 426 - Chapter 2: Site Layout and Design Guidance

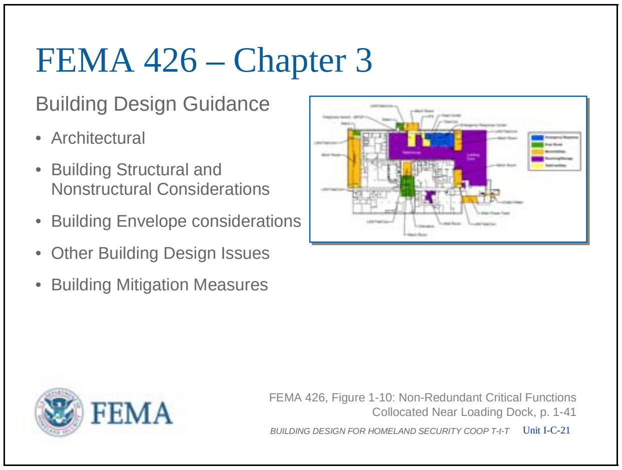
Chapter 2 discusses architectural and engineering design considerations (mitigation measures), starting at the perimeter of the property line, and includes the orientation of the building on the site. Therefore, this chapter covers issues outside the building envelope.

Chapter 2 also discusses the following site layout and design topics:

- Layout Design
- Siting
- Entry Control/Vehicle Access
- Signage
- Parking
- Loading Docks
- Physical Security Lighting
- Site Utilities

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL I-C-21



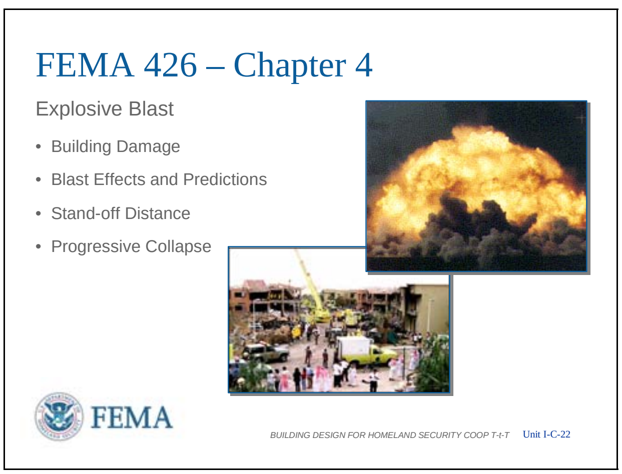
FEMA 426 - Chapter 3: Building Design Guidance

Chapter 3 provides the same considerations for the building – its envelope, systems, and interior layout.

The topic areas in Chapter 3 include:

- Architectural
- Building Structural and Nonstructural Considerations
- Building Envelope Considerations
- Other Building Design Issues
- Building Mitigation Measures

VISUAL I-C-22



FEMA 426 - Chapter 4: Explosive Blast

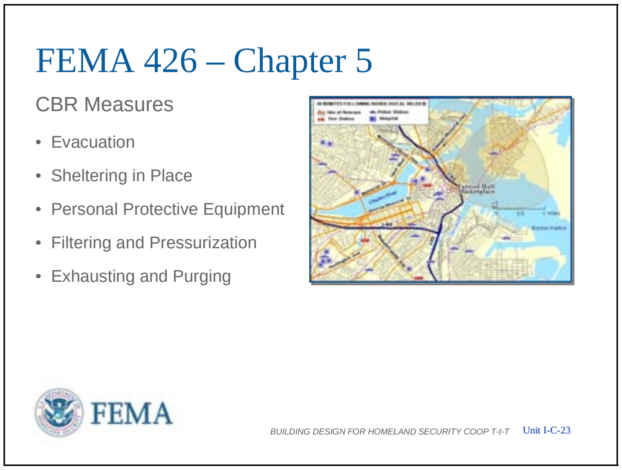
Chapter 4 provides a discussion of blast theory to understand the dynamics of the blast pressure wave, the response of building components, and a consistent approach to define levels of protection.

Some of the details you will address include:

- Building Damage
- Blast Effects and Predictions
- Stand-off Distance
- Progressive Collapse

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-23



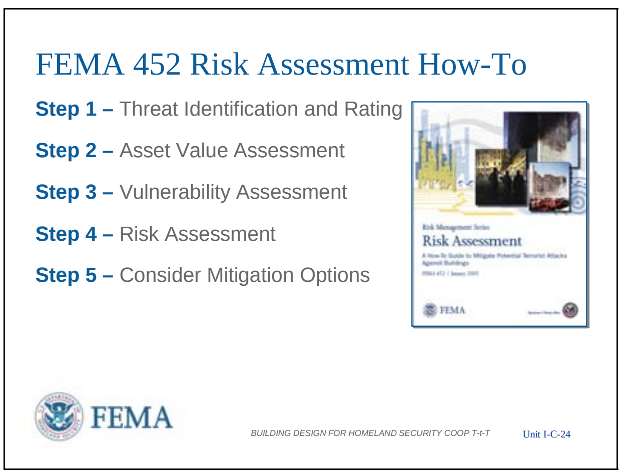
FEMA 426 - Chapter 5: CBR Measures

Chapter 5 presents chemical, biological, and radiological measures that can be taken to mitigate vulnerabilities and reduce associated risks for these terrorist tactics.

The concepts you should be familiar with at the end of the instruction include:

- Evacuation
- Sheltering in Place
- Personal Protective Equipment
- Filtering and Pressurization
- Exhausting and Purging

VISUAL I-C-24

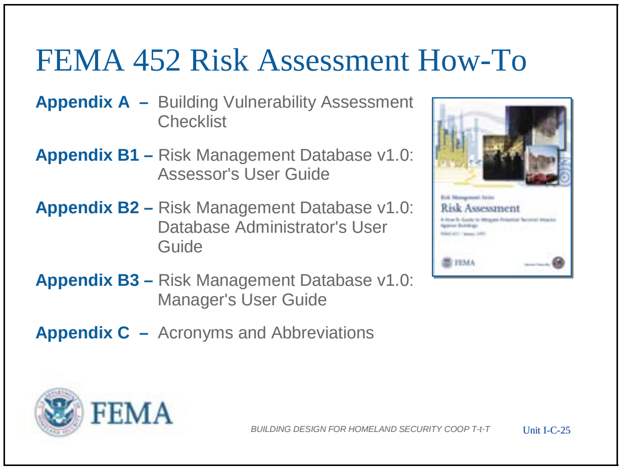


FEMA 452 Risk Assessment How-To

This publication expands Chapter 1 of FEMA 426 going into greater detail in each step of the risk assessment process as indicated by Steps 1 through 4. Step 5 takes an overarching view of mitigation options, looking at cost, benefit, special considerations, and the like, rather than going into specific mitigation options as done in Chapters 2 through 5 of FEMA 426.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL I-C-25

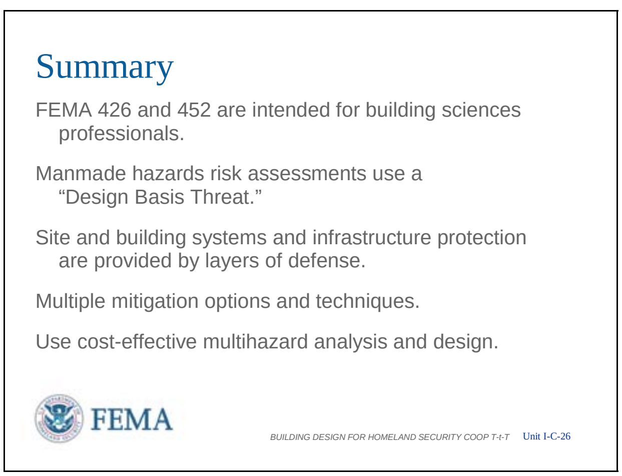


FEMA 452 Risk Assessment How-To Appendices

The manual also has five appendices to facilitate its use as a reference:

- Appendix **A** – Building Vulnerability Assessment Checklist [This is the same checklist as found at the end of Chapter 1 in FEMA 426]
- Appendices **B1, B2, and B3** – Different User Guides to use the **Version 1.0** of the FEMA 452 Risk Assessment Database that comes with FEMA 452 on the inside back cover. [This is the large organization version of the database for use on servers to facilitate access by tens and hundreds of people.]
- Appendix **C** – Acronyms and Abbreviations

VISUAL I-C-26

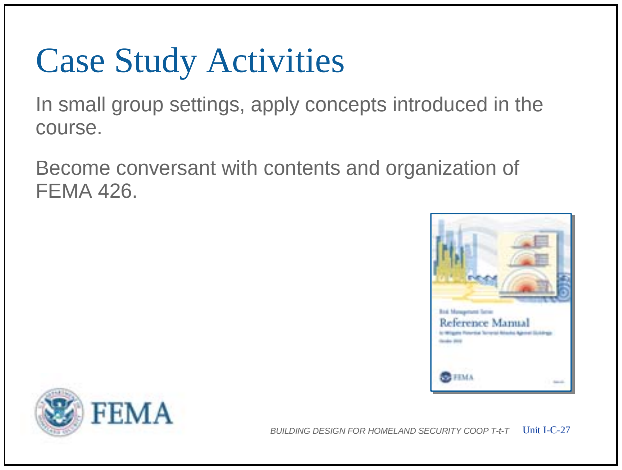


Summary

- **FEMA 426 and 452** are intended for building sciences professionals, but can be used by anyone with basic understanding of the systems being assessed.
- Manmade hazards risk assessments use a "Design Basis Threat" and "Levels of Protection" for manmade disaster and loads versus building codes for natural disaster and loads.
- Site and building systems and infrastructure protection are provided by layers of defense.
- Multiple mitigation options and techniques to deter, detect, deny, and devalue.
- Use cost-effective multihazard analysis and design.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-27

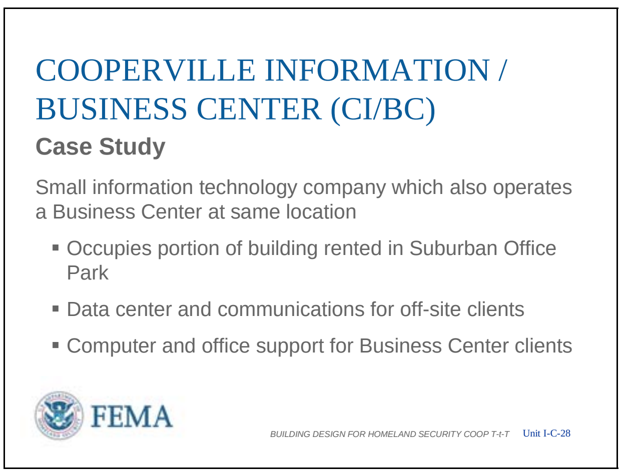


Case Study Activities

Through case studies in small group settings, students will become conversant with the contents and organization of **FEMA 426**.

- In small group settings, apply concepts introduced in the course
- Become conversant with contents and organization of FEMA 426

VISUAL I-C-28



Divide students into small groups of 5 to 8, with 7 being the optimal. Greater than 8 leaves people out of the activity and tables are not usually large enough.

Students should work in these groups for the remainder of the small group sessions.

Refer students to the Unit I Case Study activity in the Student Manual.

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

Introduction to the Case Study

The Case Study activities throughout this course provide opportunities, in a small group setting, to apply concepts introduced in each unit.

These activities will enable students to become conversant with **FEMA 426**, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*.

Students will be able to use the document readily during the process of mitigating potential damage from terrorist attacks against buildings.

The activities are designed to "walk" students through the same assessment and design steps using a Case Study involving a hypothetical building and associated data about the threat environment.

Cooperville Information / Business Center (CI/BC)

The Cooperville Information / Business Center (CI/BC) is a fictional entity created for

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

as needed.

this course (see Appendix C of the Student Manual).

- It is a composite of actual sites and buildings with actual systems typical of a number of commercial buildings.

The Case Study mainly addresses threat information related to manmade hazards:

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

Each section of the Case Study activity includes:

- Examination of specific aspects of the Case Study data.
- Assessment of data and application to the Case Study of concepts and processes addressed in the unit.
- Completion of worksheets that demonstrate participant mastery of unit learning objectives.

VISUAL I-C-29

Cooperville Information / Business Center

General Student Activity Requirements

Each student is responsible for completion of his or her own worksheets.

In addition, the small groups will <u>produce a completed worksheet for each unit's activity and post results as applicable on the Risk Matrix Poster.</u>

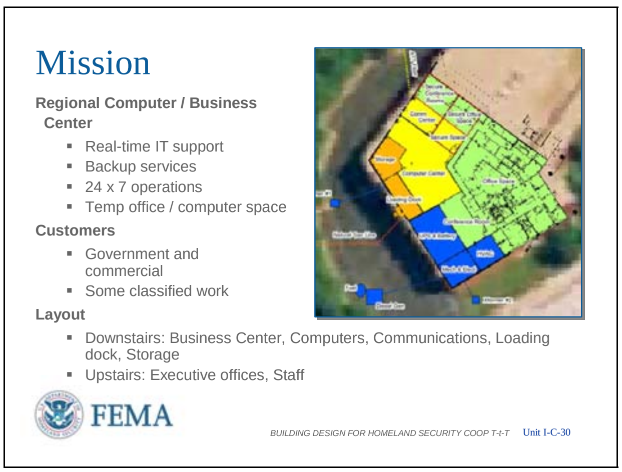
Group members are encouraged to <u>discuss activity requirements and collaborate</u> on completion of the worksheets.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

To facilitate this process, select a leader and a recorder.

- Turn to Appendix C, the COOP Case Study materials in the Student Manual and briefly peruse the document.
- Use the Case Study data to answer worksheet questions, but feel free to ask questions based upon your experience.

VISUAL I-C-30



Cooperville Information / Business Center

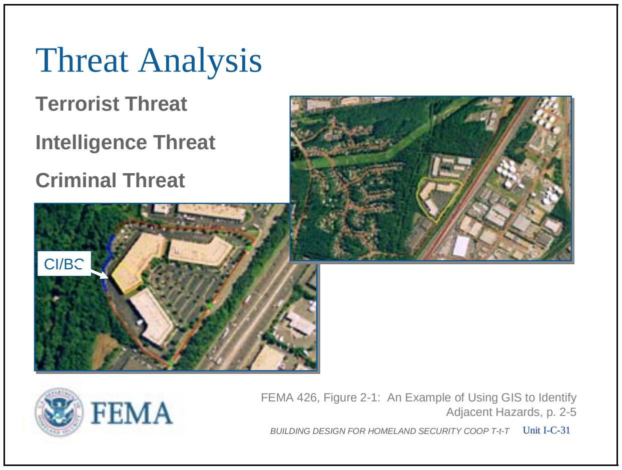
The Cooperville Information / Business Center's Information Division supports approximately 1,000 users and 100 applications as a primary data center and as a disaster recovery backup site.

The Business Center provides office space with office, telephone, and computer support for up to 82 people with unsecure office and conference room space and up to 7 people with secure office and conference room space.

CI/BC has over 75 employees and approximately 40 employees are in the building during shift changes with about 25 employees at any other time.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL I-C-31

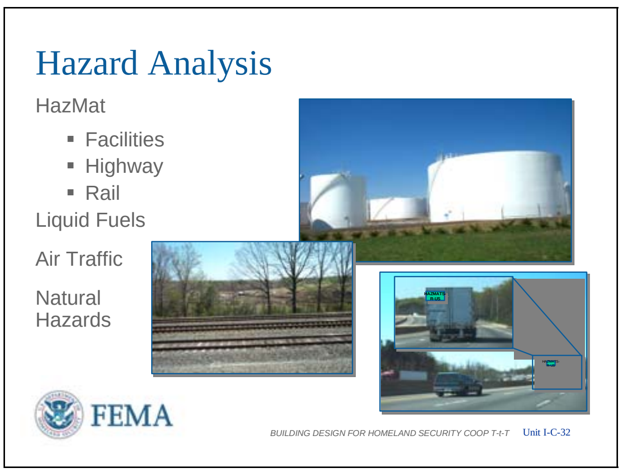


Threats/Hazards

- Terrorism
- Intelligence
- Crime

Note the site location, terrain, parking, and other commercial buildings around CI/BC.

VISUAL I-C-32



Threats/Hazards

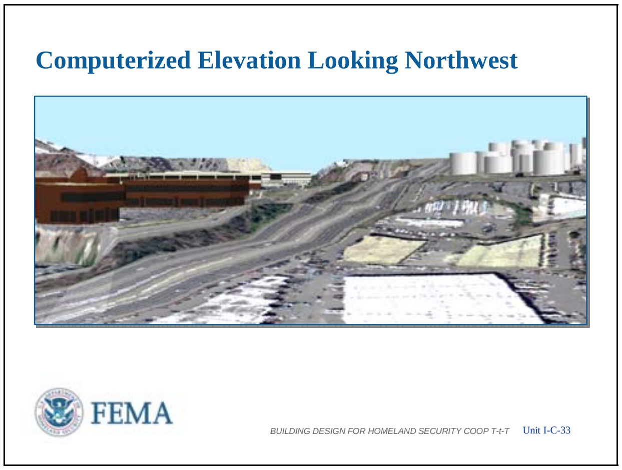
- HazMat
- Natural Hazards

Note the major interstate and rail lines near CI/BC.

Also note that from a seismic and flood standpoint, the CI/BC location (COOP alternate site) has less risk than the US Department of Artificial Intelligence primary site.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL I-C-33

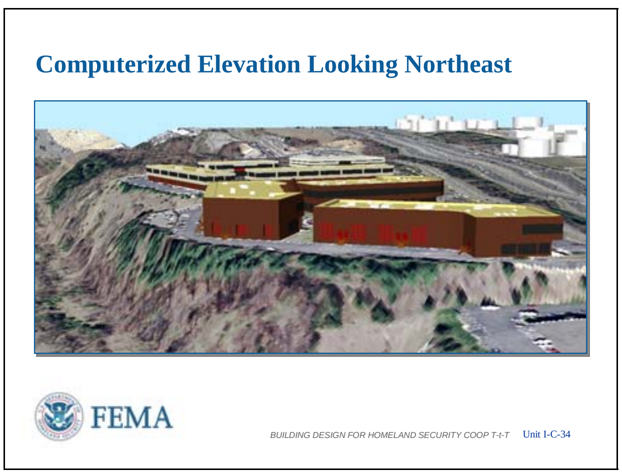


Computerized Elevation Looking Northwest

Note the elevation differences between the tank farm, the interstate, and the office park.

A tank leak overflowing the berm around the tank could flow down the interstate, but unlikely that it would flow into the office park.

VISUAL I-C-34

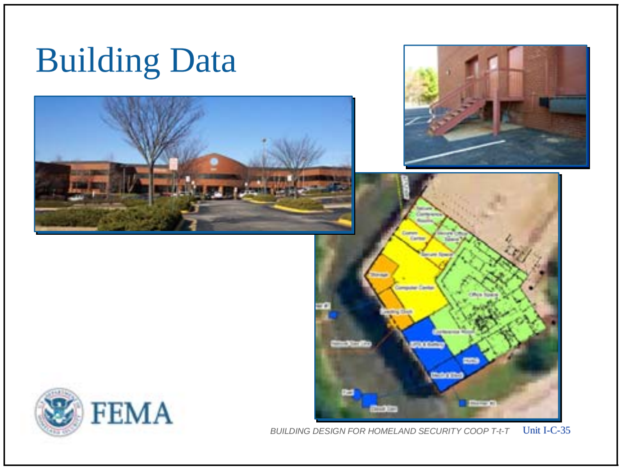


Computerized Elevation Looking Northeast

This slide shows the drop off behind the office complex which makes vehicle access very difficult from that direction.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL I-C-35



CI/BC Building Data

- Structural
- Mechanical
- Electrical
- IT
- Physical Security

Note the parking lot, building entry and exit access points, loading docks, building functions, and building infrastructure.

VISUAL I-C-36

CI/BC Building Structure

The Case Study will review the building structure and envelope to identify vulnerabilities and mitigation options.

Note the percentage of glass on the exterior walls, overhangs, and type of construction.

Also note that the interior columns have architectural standoff of about 4 inches per the graphic in the upper right corner.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

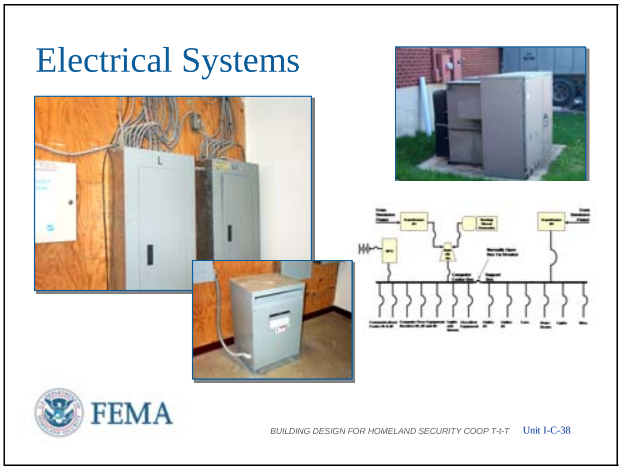
VISUAL I-C-37

CI/BC Mechanical Systems

The Case Study will review mechanical systems, plumbing, and piping to identify vulnerabilities and mitigation options.

Note the exposed meter and ground level air intake.

VISUAL I-C-38



CI/BC Electrical Systems

The Case Study will review primary electrical utilities and backup power to identify vulnerabilities and mitigation options.

Note the exposed electrical transformers, critical utility entry points, and redundancies, especially the two buss system and the tie breaker.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-39

CI/BC Physical Security

The Case Study will review physical security systems, equipment, and procedures to identify vulnerabilities and mitigation options.

Note the locations of sensors, lights, access points, and type of badges or card readers.

VISUAL I-C-40

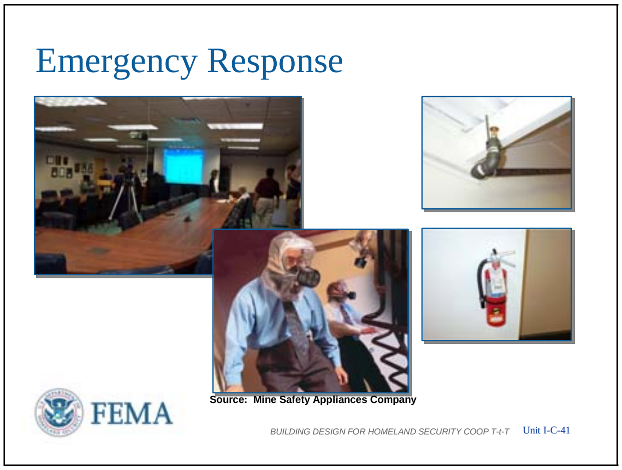
CI/BC IT Systems

The Case Study will review key IT systems to include the data center and communications to identify vulnerabilities and mitigation options.

Note the type of flooring, penetrations through the floor, mixed cable and fiber runs, and racks.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL I-C-41

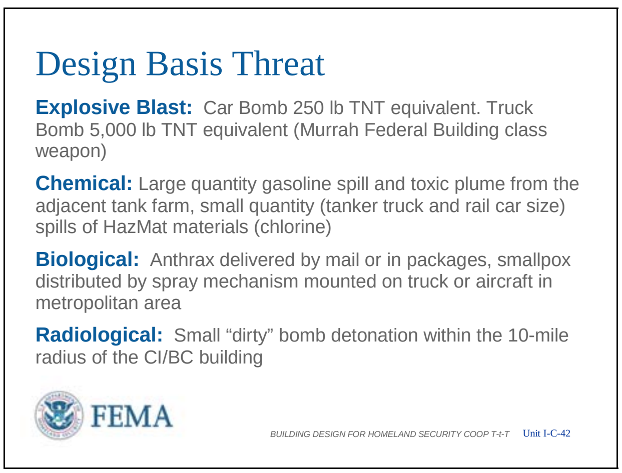


CI/BC Emergency Response

Determine the location, availability, and readiness condition of emergency response assets, and the state of training of building staff in their use.

Note the location and type of protective equipment, safe haven or shelter in place options, and mass notification capability.

VISUAL I-C-42



Design Basis Threat

- Explosive Blast
- Chemical
- Biological
- Radiological (“dirty” bomb)

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-43

Design Basis Threat

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

Cyber Attack: Focus on IT and building systems infrastructure (SCADA, alarms, etc.) accessible via Internet access

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit I-C-43

Design Basis Threat

- Criminal Activity/Armed Attack
- Cyber Attack

VISUAL I-C-44

Levels of Protection and Layers of Defense

Levels of Protection for Buildings

- Interagency Security Committee (ISC) Level II Building
- DoD Low – Primary Gathering Building

Elements of the Layers of Defense Strategy

- Deter
- Detect
- Deny
- Devalue

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit I-C-44

Levels of Protection and Layers of Defense

The Case Study will consider both the ISC and DoD Levels of Protection in order to identify vulnerabilities and to develop mitigation options.

The basic ISC and DoD Levels of Protection information is duplicated at the end of the Appendix C Case Study.

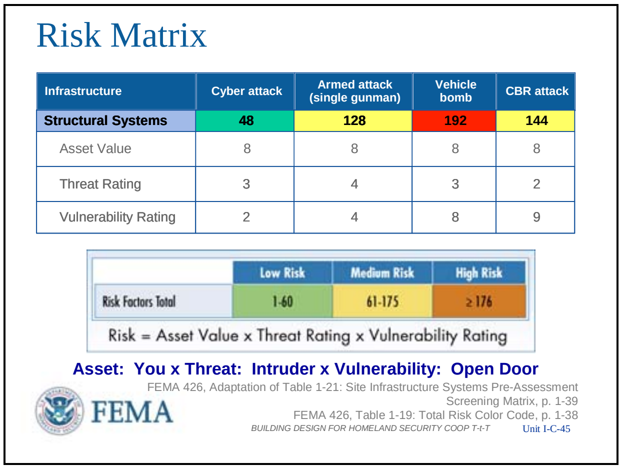
A key design strategy and concept is “Layers of Defense.” The elements of a layered system are:

- Deter
- Detect
- Deny
- Devalue

These terms are defined on page 1-9 of FEMA 426.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL I-C-45



NOTE to instructor: This is the introduction slide to how the Risk Matrix is used in the course. Do not teach the whole course on this slide. Illustrate how the Risk Matrix is used without going into ratings given as these points will be covered in subsequent instruction units.

Additional NOTE to instructor: Emphasize on this slide that FEMA 426 was built from DEFINITIONS up. That is, the General Glossary was written first as many terms have different definitions based upon the perspective of use. Asset Value, Threat, and Vulnerability are also widely defined and inconsistent between many risk assessment methodologies. In this course we will tightly define these terms in order to more easily break the risk assessment methodology into its components for ease of analysis. Thus, as shown on the slide, a simple example is that the asset it <u>YOU</u>, the threat is an <u>INTRUDER</u> attempting to get in, and the vulnerability identified is an <u>OPEN DOOR</u> between both of you that the intruder can easily use to get in and get to you.

Risk Matrix (Poster)

Whether you call the poster that you have at each of your tables [show the Poster again] a Risk Matrix or Threat Matrix or something else, its purpose as used in this course with this case study is to collect the assessment team / owner ratings and determine the highest risks that should receive the greatest attention. By splitting up the process into three logical subsets, it is easier to determine what the greatest risks are.

An example matrix from FEMA 426 indicates that the assessors and owners determined the Asset Value for the Structural Systems was 8.

Note: All ratings are on a scale of 1 – 10.

Then for each Threat the likelihood of attack upon the Structural Systems by the listed threat tactics was given a rating: 3 – 4 – 3 – 2. This was determined from a number of factors to consider.

Then the Vulnerability Rating illustrates how successful that threat tactic could fare against the Structural Systems – if the potential threat element selected that tactic to use against that asset would the potential outcome be considered successful by the terrorist or damaging by the asset owner. The vulnerability ratings listed are 2 – 4 – 8 – 9.

You will do this process for each of the entries on your Risk Matrix throughout today as you learn more about Asset Value, Threats / Hazards, and Vulnerabilities.

Then a simple calculation results in risk ratings from 1 to 1,000 in value. In this case the risk of a vehicle bomb being successfully used against the structural systems received

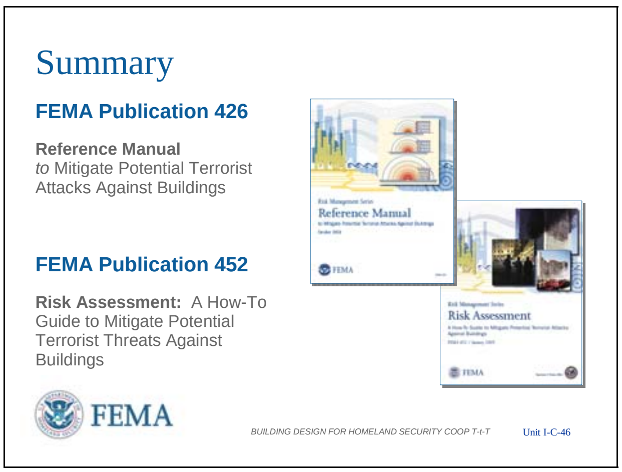
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

the highest rating (in the red "high risk" zone). You will then compare the high risk ratings to determine the highest risks that you should mitigate.

The Risk Matrix is also useful during your outbriefs on Day 3 to illustrate how your going to reduce risk for the Case Study building.

See additional NOTEs to instructor in the left column to cover on this slide.

VISUAL I-C-46



NOTE to instructor: This is a good time to emphasize students filling out the **evaluation forms** provided as feedback is important to improve this course in presentation and content.

Summary

The objective of this course is to provide a comprehensive approach to reducing the physical damage to structural and non-structural components of buildings and related infrastructure, focusing on six specific types of facilities:

- Commercial office facilities
- Retail commercial facilities
- Light industrial and manufacturing
- Health care
- Local schools
- Higher education

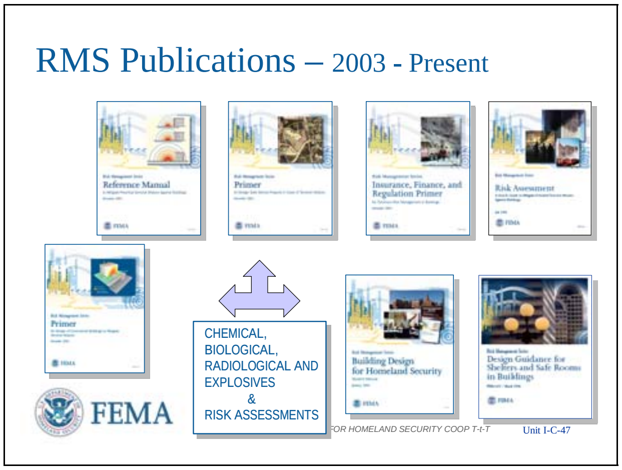
Most importantly, the course provide participants with a solid foundation on:

- Design Basis Threat
- Levels of Protection
- Layers of Defense

From a COOP standpoint, the course provides a methodology to assess COOP alternate facilities in compliance with FPC 65, including periodic reassessment.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-47



RMS Publications – 2003 – Present

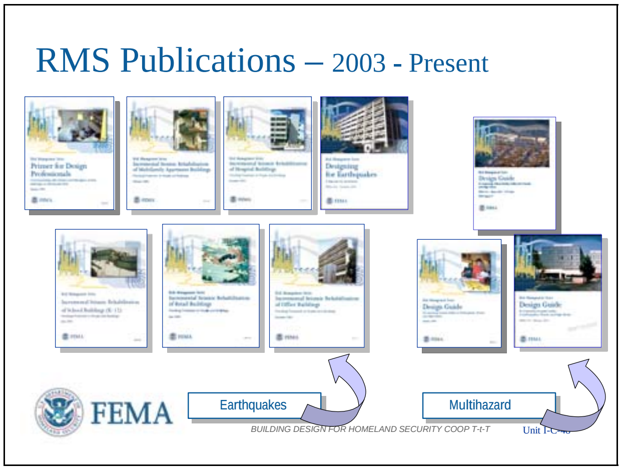
FEMA 426 and FEMA 452 are part of the Risk Management Series of publications that seek to reduce damage from natural and man-made hazards and threats.

NOTE to instructor: Do not go through the titles but they are listed here if any questions arise:

- FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 427 - Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks
- FEMA 428 - Primer to Design Safe School Projects in Case of Terrorist Attacks
- FEMA 429 - Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings
- FEMA 452 - A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 453 - Design Guidance for Shelters and Safe Rooms: Protecting People Against Terrorist Attacks
- E155 - Building Design for Homeland Security Course

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-C-48



RMS Publications – 2003 – Present

The RMS Series includes many publications dealing with specific natural hazards and multi-hazards.

NOTE to instructor: Do not go through the titles but they are listed here if any questions arise:

- FEMA 389 - Communicating with Owners and Managers of New Buildings on Earthquake Risk: A Primer for Design Professionals
- FEMA 395 - Incremental Seismic Rehabilitation of School Buildings (K-12): Providing Protection to People and Buildings
- FEMA 396 - Incremental Seismic Rehabilitation of Hospital Buildings: Providing Protection to People and Buildings
- FEMA 397 - Incremental Seismic Rehabilitation of Office Buildings: Providing Protection to People and Buildings
- FEMA 398 - Incremental Seismic Rehabilitation of Multifamily Apartment Buildings: Providing Protection to People and Buildings
- FEMA 399 - Incremental Seismic Rehabilitation of Retail Buildings: Providing Protection to People and Buildings
- FEMA 400 - Incremental Seismic Rehabilitation of Hotel and Motel Buildings
- FEMA 424 - Design Guide for Improving School Safety in Earthquakes, Floods, and High Winds
- FEMA 433 - Using HAZUS-MH for Risk Assessment: How-To Guide (not on slide)

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- FEMA 454 - Designing for Earthquakes: A Manual for Architects
- FEMA 543 - Design Guide for Improving Critical Facility Safety from Floods and High Winds

VISUAL I-C-49

RMS Publications – In Development

FEMA 452 (enhanced) – A How-To Guide to Prepare Multihazard Risk Assessments

FEMA 430 – Site and Urban Design for Security

FEMA 455 – Rapid Visual Screening for Building Security

FEMA 549 – Incremental Rehabilitation to Improve Building Security

FEMA 582 – Design Guide to improve Commercial Building Safety for Earthquake, Flood, and Wind

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit I-C-49

RMS Publications – In Development

FEMA 452 will be updated to complement the changes being made to the FEMA 452 database – COOP, Natural Hazards, and Rapid Visual Screening

FEMA 430 expands Chapter 2, Site and Layout Design Guidance in FEMA 426, using actual case studies as examples

FEMA 455 parallels the Seismic Rapid Screening approach, but for building security

FEMA 549 and 582 update previous information in the respective areas.

VISUAL I-C-50

Unit I Case Study Activity

Introduction and Overview

Background

- Answers to FEMA 452 database COOP questions applicable to Case Study found in student activity
- Note additional COOP information at end of activity

Requirements

As a team, determine if sufficient square footage is available for DAI essential functions

- Needed information contained in student activity
- Ask instructors any clarifying questions based upon your experience

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit I-C-50

Unit I Case Study Activity

Background

- The Unit 1 Student Activity in your Student Manual contains extensive additional COOP information **that is generally not part of a risk assessment.**
  - o The FEMA 452 COOP questions based upon FPC-65 requirements dealing with Deployment Planning and Alternate Facility Description are answered using Case Study information.
    - Pages SM I-C-8 to SM I-C-10
  - o The risk assessment information under Alternate Facility Description is:
    - Facility requirements for auxiliary power sources (generators)
    - Auxiliary power fuel requirement

NOTE to instructor: Point out the information in the Unit 1 Student Activity as listed in the right column. Also point out that all the information needed for determining the square footage is summarized in the Essential

INSTRUCTOR NOTES

Functions table starting on Page SM I-C-5 and totaled on Page SM I-C-6 at the end of the table. Then walk the students through the remaining content in Student Manual Unit 1. Particularly cover the Deployment Planning and Alternate Facility Description, and finish the preview by pointing out the remaining 5 documents.

NOTE to instructor: Students initially think that secure and unclassified work space is mutually exclusive, that is 18 classified cubicles and 75 unclassified cubicles are needed.

Point out the following found on Page SM I-C-3:

“**NOTE**: DAI configures their cubicles such that secure computer terminals are in secure space and the unclassified computer terminal required for these personnel are properly configured for placement in the same cubicle/workstation within the secure space.”

This means that 75-18 = 57 unclassified cubicles are needed and 18 cubicles will have both secure and unclassified computer terminals.

At the end of 20 minutes, reconvene the class and facilitate group reporting in the plenary session.

CONTENT/ACTIVITY

- Water requirement

- There are 5 additional extracts of COOP information from other FEMA sources for consideration during each student activity.
    - Pages SM I-C-11 to SM I-C-18

Requirements

- Go to the Unit I Student Activity found in your Student Manual at the Unit 1 tab and, as a group, determine if the square footage in the CI/BC Building will accommodate the US Department of Artificial Intelligence essential function during COOP use.
- All needed information is provided in the student activity
- Feel free to ask any questions dealing with any student activity if your experience indicates a different or alternate answer or concern.

Transition

In this course, you will learn how to perform a multihazard risk assessment of a building and become familiar with the key concepts to protect buildings from manmade threats and hazards:

- Asset Value
- Design Basis Threat
- Level of Protection

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

- Layers of Defense
- Vulnerability Assessment
- Risk Assessment
- Mitigation

Using the approach and guidance provided in **FEMA 426**, the majority of building owners should be able to complete a risk assessment of their building in a few days and identify the primary vulnerabilities, mitigation options, and make informed decisions on the ability of their building to survive, recover, and operate should an attack or event occur.

For the rest of the first day, the course will introduce the components of risk and how to determine risk.

- Unit II – Asset Value Assessment
- Unit III – Threat/Hazard Assessment
- Unit IV – Vulnerability Assessment
- Unit V – Risk Assessment/Risk Management

UNIT I (C) CASE STUDY ACTIVITY: CASE STUDY OVERVIEW (COOP Version)

Requirements

SQUARE FOOTAGE ANALYSIS – Does the CI/BC Building have sufficient space to accommodate the DAI essential functions?

NOTE to instructor: The ***blue bold italics*** information below is the school solution for this student activity. All other information is provided to the students.

Criteria used to evaluate square footage (rules of thumb):
Workstations in Business Center office areas average 100 square feet in floor space. Additional workstations or tables are available on a one-day's notice.

There is no formal Federal Government-wide standard for office space per person. However EPA and GSA recommend 225-230 usable square feet per person which includes all individual and shared space such as workstations, circulation, storage, filing space, and conference rooms. The minimum functional workstation footprint is 64 to 80 square feet (an 8 foot by 8 foot to 8 foot by 10 foot cubicle).

A good approach is to use 100 square feet as the minimum space needed for each work station to allow for movement around office and filing/storage space for deployed equipment and files.

a. Available Unclassified Square Footage for Personnel: ***8,225 or 8,775 (w/half of Conf Room)***

(1) Shift Personnel Requiring Unclassified Square Footage: ***57***
(with **no** secure computer terminal co-located)

NOTE: DAI configures their cubicles such that secure computer terminals are in secure space and the unclassified computer terminal required for these personnel are properly configured for placement in the same cubicle/workstation within the secure space.

See Page SM I-C-8 for Alternate Facility Description Personnel Shift Configuration

There are 75 total COOP personnel on shift at any one time. It is assumed that all shift personnel requiring secure computer terminals (18 out of the 75) will be in a secure space and their unclassified computer terminals would be available at the same location using a selector switch or separate terminals. Other approaches would require unclassified terminals to be outside the secure spaces, but in that case a one-to-one person-to-unclassified computer relationship would not be

needed for those in secure spaces and 6 unclassified terminals would be more than adequate and the space required for these unclassified terminals would not be anywhere near 80 square feet. Thus, unclassified space is only required for those who have no secure computer requirements and that number is 75-18 = 57.

(2) Minimum Required Unclassified Square Footage for Personnel: __***5,700***___

(3) Maximum Required Unclassified Square Footage for Personnel: _***13,110***____

(4) Available Unclassified Square Footage per person: __***144.3 to 153.9***___

Business Center Office Space – 11,000 SF
Includes Main Conference Room – 1,100 SF which can be partitioned in half
Includes Secure Office Space – 745 SF
Includes Secure Conference Rooms – 930 SF
Business Center Office Space (Unclassified) = 11,000 – 745-930-1,100 = 8,225 SF office space available

1. ***At 100 SF/Workstation the Business Center is set up to support 82 personnel (8,225 / 100)***
2. ***Using EPA/GSA 230 SF/person requires 230 x 57 = 13,110 SF (not enough SF)***
3. ***Minimum of 100 SF/person requires 5,700 SF (more than enough, but configuration may be unattainable)***
4. ***Unclassified SF/Person = 8,225 / 57 = 144.3 SF***
5. ***No problem with Unclassified Office Square Footage. Could use half of main conference room if needed additional space due to workstation layout.***

b. Available Secure (Classified) Square Footage for Personnel: _***1,675 or 2,275 (w/InfoDiv space)***__

(1) Shift Personnel Requiring Secure Square Footage: ___***18***_____
(with unclassified computer terminal co-located)

See Page SM I-C-8 for Alternate Facility Description Personnel Shift Configuration

(2) Minimum Required Secure Square Footage for Personnel: __***1,800***___

(3) Maximum Required Secure Square Footage for Personnel: ___***4,140***__

(4) Available Secure Square Footage per person: __***93 to 126.4 (using all secure space)***___

Business Center Secure Office Space – 745 SF
Business Center Secure Conference Rooms – 930 SF
Information Division Secure Space – 600 SF

1. ***At 100 SF/Workstation the Business Center is set up to support 7 secure personnel (745 / 100) using only Business Center secure office space***
2. ***At 100 SF/Workstation the Business Center can support 16 secure personnel using the Secure Office Space (7 personnel) and the Secure Conference Rooms (9 personnel).***
3. ***Thus, DAI must use the Information Division Secure Space to cover the 18 personnel. 7 + 9 + 6 = 22 personnel (total capability using existing configuration)***
4. ***Using EPA/GSA 230 SF/person requires 230 x 18 = 4,140 SF (not enough SF)***
5. ***Thus, additional workstations, including computers and telephones, need to be moved into the Secure Conference Room space within 24 hours after notification of the COOP activation or 12 hours with preplanning and locally stored workstations and equipment.***

BACKGROUND INFORMATION

The needed information from Appendix C, Case Study, is contained here to answer the square footage questions. Use only the Case Study data to answer the student activity questions. However, feel free to ask questions of the instructors based upon your experience.

ESSENTIAL FUNCTIONS – NOTE: Table information is summarized in the last row of the table.

Priority	Essential Function	Req Square Footage	Req # Personnel	Req # Computer Terminals (U) Unclassified (S) Secure	Req # Telephones (U) Unclassified (S) Secure	Req Cell Phone Coverage (Y or N)
1	Orchestrate national level response to any loss of artificial intelligence production capability and loss of AI revenue required for payments to US citizens		4 COOP Site Managers 10 Staff	(U) 2 (U) 5 (S) 5	(U) 2 (S) 5	Y 4 N
2	Consult with and provide reports and other technical assistance to appropriate Federal agencies that may be impacted by loss of AI component availability and resultant revenue flow		4 COOP Site Fin Sys Mgrs 12 Staff	(U) 2 (U) 6 (S) 6	(U) 2 (S) 6	Y 4 N
3	Process and post financial documents supporting monthly cash flow to Agencies that distribute AI		36	(U) 18	(U) 18	N

Priority	Essential Function	Req Square Footage	Req # Personnel	Req # Computer Terminals (U) Unclassified (S) Secure	Req # Telephones (U) Unclassified (S) Secure	Req Cell Phone Coverage (Y or N)
	revenues to entitlement recipients					
4	Operate personnel / payroll system to ensure all DAI personnel receive payments		28	(U) 14	(U) 14	N
5	Manage operations, security, safety, and health programs for all DAI personnel, programs, and operations		20	(U) 10 (S) 2	(U) 10 (S) 2	Y-4
6	Manage Department-wide computer security functions		10	(U) 5 (S) 5	(S) 5	N
7	Provide liaison with state, local, and tribal officials on status of critical AI production, availability, and shortfalls.		26	(U) 13	(U) 13	Y 5
	Summary of Essential Function Requirements		Mgrs 8 Staff 142	(U) 75 (S) 18	(U) 59 (S) 18	17

ADDITIONAL INFORMATION – Consider during each student activity throughout course.

FEMA 452 COOP questions – answered

1. Deployment Planning
2. Alternate Facility Description

Information from other FEMA sources:

3. FEMA 452 Risk Assessment Database v3.0, Checklist Questions – Section 14 COOP Facility: Additional Concerns
4. Glossary of COOP terminology, FEMA Independent Study (IS) 546, *Continuity of Operations (COOP) Awareness Course.*
5. Alternate Facility Selection Factors, FEMA IS 547, *Introduction to Continuity of Operations.*
6. Components of an Effective Vital Records Program, FEMA IS 547.
7. FPC-65 Testing Requirements.

2. DEPLOYMENT PLANNING

a. Minimum distance to alternate facility ____60____ miles.

b. Required access to transportation:

_____?____ Yes/No Privately Owned Vehicle

_____?____ Yes/No Agency Arranged Transportation

_____?____ Yes/No Mass Transit

Types of Mass Transit at Primary Facility:

___Yes____ Yes/No Bus

___Yes____ Yes/No Rail

___Yes____ Yes/No Taxis

Types of Mass Transit at Alternate Facility:

___Yes____ Yes/No Bus

___Yes____ Yes/No Rail

___Yes____ Yes/No Taxis

3. Alternate Facility Description:

a. How soon after decision to deploy must site be available?
___12_____ # of hours

b. Number of Persons to be supported overall (all shifts) ___150___ # people

Shift ___A_____ Number of Persons on shift ___75_____ # people

Shift ___B_____ Number of Persons on shift ___75_____ # people

Shift _________ Number of Persons on shift __________ # people

c. When this alternate facility is activated, how many hours per day and days per week will it operate?

____24____ # hours per day

____7_____ # days per week

d. If people must stay overnight at the site, indicate the total billet requirement.

____150______ # billets per day

Where will billets be located?

There is sufficient hotel room space in the local area to handle part or all of the Emergency Relocation Group. Local colleges can be contacted for use of dormitory space, but this would be limited to the summer months per a preliminary inquiry.

e. If necessary, the number of meals served on site per day?

____150___ # of meals per day

How will meals will be provided, and for what meals (breakfast, lunch, dinner, and for which shift)?

Local eateries are not 24 hour operations, thus the lunch meal on the night shift will need to be catered and, for consistency, the lunch meal on the day shift should also be catered. Breakfast and dinner for both shifts are at the discretion of the individual prior to starting shift and after ending shift. There are many caterers/delicatessens/restaurants in the local area that could provide a variety of delivered foods for one or both meals.

f. Facility requirements for auxiliary power sources (generators)

___1,500 KVA___ power requirement (maximum)

___1,000 KVA___ critical load (on UPS)

___1250 eKW / 1563KVA___ generator capability/capacity

___26 hours___ duration (hours, days, weeks) (minimum)

Based upon the refueling of the fuel tank(s) each day (24 hours). Recommend ensuring there are at least 3 fuel suppliers in different localities to ensure servicing of the fuel tank during any power outage contingency.

g. Auxiliary power fuel requirement

Estimating Rule of Thumb: 0.08 gallons / KW / hour

___100___ # gallons per hour (1250 KW x 0.08 gallons / KW / hour)

___22 hours___ duration capability (full tanks – hours, days, weeks) (with day tank 80% full)

Increase fuel capacity with another tank or use a portable tank during the peak summer months when the maximum load is expected to occur. Alternately, during an exercise ensure this COOP site is fully functional and measure actual load to better understand consumption and duration capability. Adjust capacity requirements accordingly.

h. Parking requirement

___0___ Unsecured stalls

___0___ Secured stalls

447 in front & 155 in rear Total stalls available (therefore no parking problem even if all Emergency Relocation Personnel bring a POV)

i. Vehicle fuel requirement

___0___ # gallons per day ***(all vehicles to be refilled at local gas stations)***

j. Water requirement

___112.5 to 22,500___ # gallons per day

Estimating Rules of Thumb:
2-quarts - 2 gallons per person per day for consumption/minimal washing
50 gallons / person / day for personal use (drinking, washing, flushing, food prep)
100 gallons / person / day for all building uses
150-160 gallons / person / day for water production
Cooling Tower evaporates 3 gallons / minute / 100 tons of air conditioning or 4,320 gallons per day / 100 tons of air conditioning. Cooling Tower sumps for these size units contain 150-300 gallons. Thus without water supply, cooling towers can last about 50-100 minutes before they have insufficient water to operate properly (piping not filled)

Estimated consumption using Rules of Thumb:
75 CI/BC employees + 150 Emergency Relocation Group personnel = 225
225 persons x 0.5 = 112.5 gallons / day minimum for consumption/minimal washing
225 persons x 100 = 22,500 gallons / day for all building uses

Available water if water main shut off:
Bottled water = 5 dispensers x 3 spare jugs x 5 gallons per jugs = 75 gallons, up to 100 gallons if each dispenser has a new jug.
NOTE: Will have to arrange additional bottled water and reserves to supply COOP operation.

k. Radio requirement

None

l. Satellite communication requirement

A satellite link is needed for secure and non-secure worldwide communications as a backup to telephone landlines. This may already be in the ERG Office Go Kit.

m. Other requirement

None listed.

3. FEMA 452 Risk Assessment Database v3.0
Checklist Questions – Section 14 COOP Facility: Additional Concerns

14-1: **Essential Functions**: Have the essential functions been identified and prioritized to establish the planning parameters for the alternate operating facility?

14.2: **Essential Functions**: Have reliable processes and procedures been established to acquire resources necessary to continue essential functions and sustain operations until normal business activities can be reconstituted, which could be up to 30 days?

14-3: **Communications**: Does the alternate operating facility provide interoperable communications, including a means for secure communications, with all identified essential internal and external organizations, customers, and the public?

14-4: **Communications**: Have the internal and external communications capabilities at the alternate operating facility been validated quarterly?

14-5: **Communications**: Does the COOP facility have wireless / cell phone capability? Have wireless and cell phone providers been reviewed and compared to ensure the best service is provided? Are services available / compatible within the building to support essential functions and missions?

14-6: **Test, Training, and Exercises**: Has there been annual testing of primary and backup infrastructure systems and services at alternate operating facilities (e.g., power, water, fuel)?

14-7: **Test, Training, and Exercises**: Have physical security capabilities been tested / exercised annually and shown to able to be in place within 12 hours of COOP plan activation?

14-8: **Planning Requirements**: Is the alternate operating facility located in an area where power, telecommunications, and internet grids are distinct from those of the primary facility?

14-9: **Planning Requirements**: Is the distance between the primary facility and the alternate operating facility sufficient to allow it to continue essential agency functions?

14-10: **Planning Requirements**: Has the organization identified which essential services and functions that can be continued from remote locations (e.g., home facilities or other alternative workplaces) and those that need to be preformed at a designated department or agency operating facility?

14-11: **Planning Requirements**: Does the alternate facility have detailed site preparation and activation plans or have pre-positioned supplies and resources in order to achieve full operational capability within 12 hours of notification?

14-12: **Planning Requirements**: Is the COOP facility able to accommodate all emergency relocation group members in a safe and efficient manner?

14-13: **Planning Requirements**: Does the COOP facility contain the sufficient amount of phones, computers, and necessary equipment needed to sustain COOP operations?

14-14: **Vital Records**: Has the organization identified vital records needed to perform its essential functions during a COOP event?

14-15: **Vital Records**: Do emergence response group members have access to their vital records at the alternate facility? Are they available within 12 hours or less of a COOP plan activation.

14-16: **Vital Records**: Are periodic review / updates of the vital records program conducted to address any new security issues, identify problem areas, and identify additional vital records that may result from new agency programs or functions?

14-17: **Vital Records**: Are there separate COOP servers? Are they placed in a secure area? Are there backup procedures?

14-18: **Vital Records**: Has a risk assessment of vital records been performed to determine:

a. Identify risks involved if vital records are retained in their current location and medium, and the difficulty reconstituting them if they are destroyed.

b. If off site storage is necessary?

c. Determine if alternative storage media is advisable?

d. Determine if it is necessary to duplicate records to provide a vital records copy?

14-19: **Human Capital**: Is adequate Personal Protective Equipment available for all emergency response group members while on-site?

14-20: **Human Capital**: Are there sufficient quantities of Personal Protective Equipment for emergency response group members to sustain operations for 30 or more days?

14-21: **Human Capital**: Are medical facilities, proper caregivers, and first aid kits available for emergency response group members if and when needed?

14-22: **Human Capital**: Is there access to essential resources such as food, water, fuel, and municipal services at the facility?

14-23: **Security**: Does the site provide physical security that meets all requirements established by annual threat assessments and physical security surveys?

4. Glossary of COOP Terminology
FEMA Independent Study (IS) 546
Continuity of Operations (COOP Awareness Course

Alternate communications: Provide for the capability to perform essential functions, in conjunction with other agencies, until normal operations can be resumed.

Continuity of Government Plans: Developed and implemented in the event of a catastrophic emergency to ensure that our government continues to exist and function.

Continuity of Operations: A Federal initiative, required by Presidential Directive, to ensure that Executive Branch departments and agencies are able to continue their essential functions under a broad range of circumstances.

Delegations of Authority: Formal documents that specify who is authorized to act on behalf of the agency or other key officials for specific purposes.

Devolution: The capability to transfer statutory authority and responsibility for essential functions from an agency's primary operating staff and facilities to other employees and facilities.

Essential Functions: Those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public, and sustain the industrial or economic base during an emergency. Essential functions must continue with no or minimal disruption.

Exercises: Events that allow participants to apply their skills and knowledge to improve operational readiness. Exercises also allow planners to evaluate the effectiveness of previously conducted tests, training, and exercises.

Federal Preparedness Circular 65: Issued by FEMA to provide specific and detailed guidance regarding COOP capabilities.

Full-Scale Exercise: Test the agency's total response capability for COOP situations. These exercises are as close to reality as possible, with personnel being deployed and systems and equipment being implemented.

Functional Exercise: Simulate a function (e.g., alert, notification) within a real incident. Functional exercises test a single part of COOP activation to be tested independently of other responders.

"Go Kit": A kit that should be assembled by each employee and his or her family and should include personal items and necessities, financial and legal documents, and the name and phone number of an out-of-area contact.

Hands-On Training: Can provide practice in specialized skills (e.g., notification procedures), allow for practice of newly acquired skills, and help maintain proficiency at infrequently used skills.

Multi-Year Strategy and Program Management Plan: The long-term plan for keeping the COOP up to date.

Occupant Emergency Plans: Intended to ensure the safety of personnel in the event of an incident inside or immediately surrounding an agency's building.

Orders of Succession: Provide for the orderly and predefined assumption of senior agency offices during an emergency in the event that any officials are unavailable to execute their legal duties. All orders of succession should include the conditions under which succession will take place, the method of notification, and limitation on delegations of authority by successors.

Orientations: The first type of training conducted in an exercise program. Orientations are usually conducted as briefings and are a good way to introduce the general concepts of a COOP plan; announce staff assignments, roles, and responsibilities; present general procedures; and describe how the COOP plan will be tested and exercised and within what timeframes.

Presidential Decision Directive 67: Issued by former President Bill Clinton, requiring all Federal departments and agencies to develop plans in response to all hazards and a full spectrum of threats.

Reconstitution: The process by which surviving and/or replacement agency personnel resume normal agency operations from the original or replacement primary facility.

Relocation: Involves the actual movement of essential functions, personnel, records, and equipment to the alternate operation facility. Relocation may also involve transferring communications capability to the alternate facility, ordering supplies and equipment that are not already in place at the alternate facility, and other planned activities, such as providing network access.

Tabletop Exercise: A simulation activity in which a scenario is presented and participants in the exercise respond as if the scenario was really happening.

Test: An evaluation of a capability against an established and measurable standard.

Test, Training, and Exercise Program (TT&E): Includes measure to ensure that an agency's COOP program is capable of supporting the continued operation of its essential functions throughout the duration of a COOP situation. TT&E program should be a blend of test, training, and exercise events to ensure that it is comprehensive in that it includes all three components and reflects lessons learned from previous TT&E events.

Training: Instruction in core competencies and skills and is the principal means by which individuals achieve a level of proficiency.

Vital Records: Records that are vital to an agency and its operations. The records include emergency operating records and legal and financial records.

5. Alternate Facility Selection Factors
FEMA Independent Study (IS) 547
Introduction to Continuity of Operations

Factor	Explanation
Location	Select a site that provides a risk-free environment, if possible, and is geographically dispersed from the primary work location. This will reduce the chance that the site will be affected by the same event that required COOP activation.
Construction	The alternate facility should be constructed so that it is relatively safe from the high-risk hazards in the area.
Existence of an MOU/MOA	The General Services Administration may have space available that is suitable for an alternate facility. Another option may be to enter into a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) with another agency to share space during COOP activation.
Space	The alternate facility must have enough space to house the personnel, equipment, and systems required to support all of the organization's essential functions.
Billeting and Site Transportation	Billeting and site transportation should be available at or near the alternate facility. Sites that are accessible by public transportation and that provide billeting or are near hotels offer important advantages.
Communication	The site will need to support the agency's COOP information technology and communication requirements. The agency will need to acquire any capabilities not already in place.
Security	Security measures, such as controlled access, should be an inherent part of the alternate facility.
Life Support Measures	Access to life support measures—food, water, and other necessities—should be available onsite or nearby.
Site Preparation Requirements	The amount of time, effort, and cost required to make the facility suitable for the agency's needs is critical. The more "turnkey" the facility is, the better.
Maintenance	Consider the degree of maintenance required to keep the facility ready for COOP operations. Lower-maintenance facilities offer a distinct advantage in case of no-warning COOP activation.

6. Components of an Effective Vital Records Program
FEMA Independent Study (IS) 547
Introduction to Continuity of Operations

Component	Description
Vital Records Directive	A directive from senior leadership that establishes the vital records program and assigns responsibility for vital records management. The directive should: Specify the purpose and scope of the program. Assign roles and responsibilities. Provide for staff training. Require periodic review and testing of the program.
Appropriate Medium	The determination of an appropriate medium for each type of vital record to enable the Emergency Relocation Group (ERG) to access the records within 12 hours, or less, as required, of activation. Agencies should strongly consider: Multiple redundant media for storage of vital records. Methods to facilitate the rapid recovery of records necessary to ensure business survival.
Records Inventory	A complete inventory of the records identified as vital to agency operations. The inventory should include: The **location** of the records. Complete **access information**.
Risk Assessment	An assessment that: Identifies the risks involved if the vital records are retained in their current locations and in their current media—and the difficulty of reconstituting them if they are destroyed. Determines the level of physical security and confidentiality of the records. Determines offsite storage—perhaps in a regional office or in commercial storage. Identifies whether alternate storage media are advisable. Determines whether duplication may be required for records that will be stored off site, are static, or are available in hardcopy only.

Records Protection Methods	The selection of appropriate protection methods for all vital records, including whether: Dispersal to other locations may be required. If records are to be dispersed, the site must have controlled access separately from the site where the records were created or used regularly. Special media protection methods are required.
Update Procedures	Procedures for routinely updating vital records so that they always contain the most current information.
Recovery Strategy	The identification of records recovery experts and vendors who can assist with the recovery of vital records in the event of damage or loss.
Vital Records Packet	A packet that includes: A list of key personnel and disaster staff including up-to-date telephone numbers or other contact information. A complete inventory of the vital records and their precise locations. Necessary keys and/or access codes for the records. The locations of alternate operating facilities. The packet should be reviewed periodically to ensure that the information is current.
Training	A training program for all staff involved in the vital records program. Training for vital records should focus on the vital records policies and procedures as well as personnel responsibilities.
Review Program	A strategy for periodic review of all vital records. The program should: Address new security issues that have been identified since the last review. Update information in the vital records as necessary. Identify additional vital records. Provide an opportunity to familiarize staff with the program.
Testing Capabilities	A testing strategy that evaluates capabilities for: Protecting classified and unclassified vital records and databases. Providing access to vital records from alternate facilities. Testing is required semiannually.

7. FPC-65 COOP Testing Requirements

(Potential impact on alternate facility indicated by ***bold italics***)

Testing is an important part of COOP readiness. By testing, agency personnel can tell if the policies and procedures work as they should, when they should. Testing is critical for:

Alert, notification, and ***activation procedures***.

Communications systems.

Vital records and databases.

Information technology systems.

Major systems at the alternate facility (e.g., power, water).

Reconstitution procedures.

FPC-65 requires testing of certain aspects of the COOP plan. The agency test program must include:

Quarterly testing of alert, notification, and ***activation procedures***.

Semiannual testing of plans for the recovery of vital classified and unclassified records and critical information systems, services, and data.

Quarterly testing of communications capabilities.

Annual testing of primary and backup infrastructure systems and services at alternate operating facilities (e.g., power).

This page intentionally left blank

Unit II (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 75 minutes
UNIT TITLE	Asset Value Assessment
OBJECTIVES	1. Identify the assets of a building or site that can be affected by a threat or hazard 2. Explain the components used to determine the value of an asset 3. Determine the critical assets of a building or site 4. Provide a numerical rating for the asset and justify the basis for the rating
SCOPE	The following topics will be covered in this unit: 1. The core functions and critical infrastructure listed on the threat-vulnerability matrix. 2. Various approaches to determine asset value – FEMA, Department of Defense, Department of Justice, and Veterans Affairs. 3. A rating scale and how to use it to determine an asset value. 4. Activity: For the assets identified in the Risk Matrix, use the information in the Case Study, review the asset value for each asset of interest, and provide rationale for the asset value rating given.
REFERENCES	1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-10 to 1-14 2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 2-1 to 2-26 3. Case Study – Appendix C: COOP, Cooperville Information / Business Center 4. Student Manual, Unit II (C) (info only – not in SM) 5. Unit II (C) 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 II (C)
4. Student Manual COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit II (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

UNIT II (C) OUTLINE

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 asset value. Also, the determination of asset value rating is subjective because this course was designed for small organizations with few decision makers or levels of decision making. Large organizations would need a more objective approach to asset value rating so that the ratings of different people would be comparable, which does not occur in small organizations.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will apply the techniques of asset identification and asset value rating to the Case Study in order to identify and rate the assets found in the Case Study. The students will have to quickly scan the Case Study information with the specific intent of determining assets and their value to the organization. Reading the Case Study prior to the class greatly helps in performing this activity.

- Refer students to their Student Manuals for worksheets and activities.
- Direct students to the appropriate page (Unit #) in the Student Manual.
- Instruct the students to read the activity instructions found in the Student Manual. Note that this Student Activity provides asset value ratings that the students must determine agreement with and rationale for the given asset value rating.
- Explain that the asset value 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.

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

(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

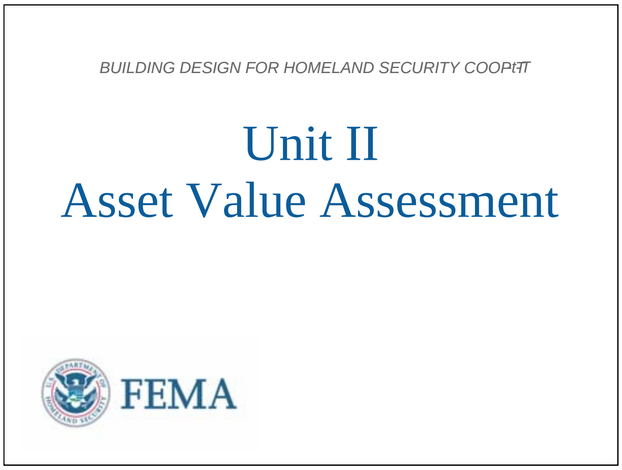
(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL II-C-1



Introduction and Unit Overview

This is Unit II, Asset Value Assessment. This section will describe how to perform an asset value assessment (the first step in the assessment process), to identify people and asset values categorized as core functions and core infrastructure. Key to this process is interviewing stakeholders including owners, facility staff, and tenants.

VISUAL II-C-2

Unit Objectives

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

1. Identify the assets of a building or site that can be affected by a threat or hazard.

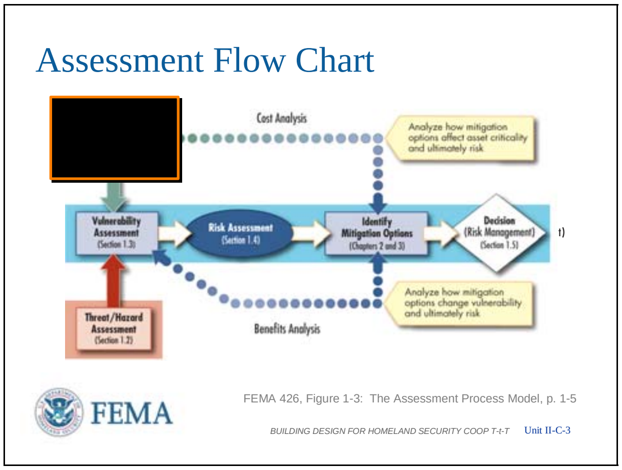
2. Explain the components used to determine the value of an asset.

3. Determine the critical assets of a building or site.

4. Provide a numerical rating for the asset and justify the basis for the rating.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-C-3

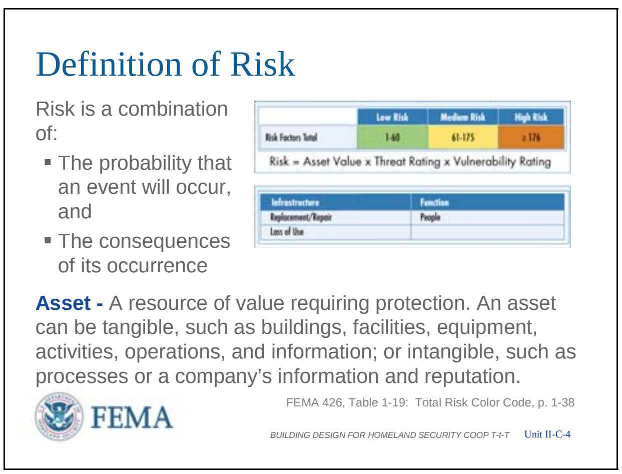


Assessment Flow Chart

Reviewing the Assessment Flow Chart, the first step in the risk assessment process is to determine asset value.

An asset is anything you want to protect because of its value, its need to maintain business continuity, and/or its difficulty in replacing within a required timeline.

VISUAL II-C-4



Risk

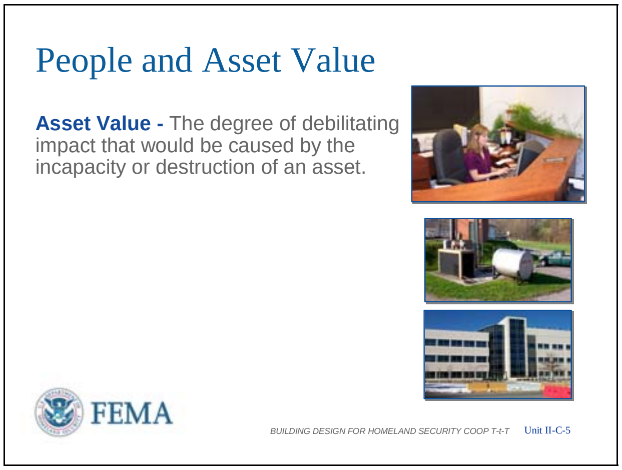
Risk can be defined as the potential for loss of or damage to an asset. It takes into account the **value of an asset**, the **threats or hazards** that potentially impact the asset, and the **vulnerability** of the asset to the threat or hazard.

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

In general terms, asset value can be considered the replacement cost for infrastructure and equipment. It can include lost profit to a business or lost capability to a mission that result in greater damage and loss to that asset and other assets.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-C-5



People and Asset Value

Understanding asset criticality is comparable to strategic planning in that the building owner should understand the mission of the organization, the resources that are used to perform that mission, how those resources interface with one another to achieve goals, and how the organization would cope or maintain business continuity if the asset(s) were lost.

People are a building's most critical asset.

VISUAL II-C-6

Identification of a Building's Assets

Identifying a building's critical assets is accomplished in a two-step process.

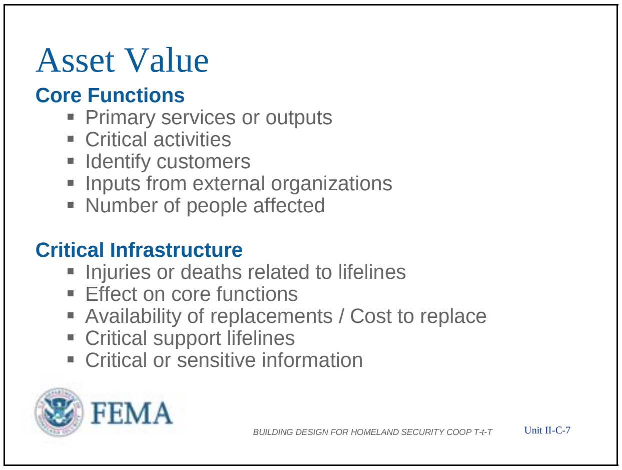
Step 1: Define and understand a building's core functions and processes.

Step 2: Identify site and building infrastructure and systems:

- Critical components/assets
- Critical information systems and data
- Life safety systems and safe haven areas
- Security areas

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-C-7



Asset Value

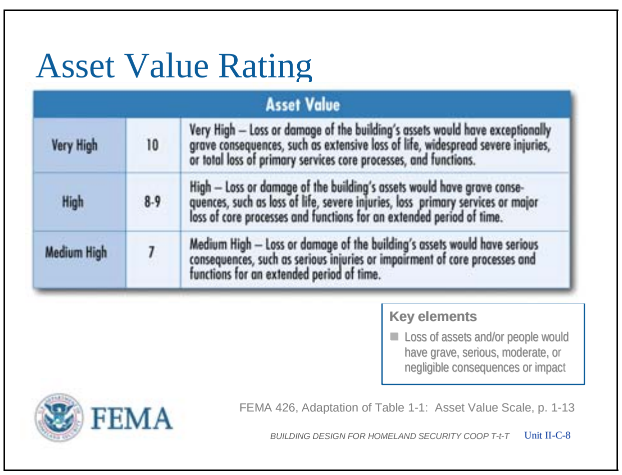
The objective in the initial step is to determine the core functions for the building that will enable it to continue to operate or provide services after an attack. This focuses the assessment team on the key areas of the building. Factors include:

- What are the primary services?
- What critical activities take place at the building?
- Who are the building's occupants and visitors?
- How many people are affected by the loss of this asset

To help evaluate and rank critical infrastructure, consider the following factors:

- Injuries or deaths related to critical infrastructure damage
- Effect on core functions
- Availability of replacements / Cost to replace
- Critical support lifelines
- Critical or sensitive information

VISUAL II-C-8



Asset Value		
Very High	10	Very High – Loss or damage of the building's assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services core processes, and functions.
High	8-9	High – Loss or damage of the building's assets would have grave consequences, such as loss of life, severe injuries, loss primary services or major loss of core processes and functions for an extended period of time.
Medium High	7	Medium High – Loss or damage of the building's assets would have serious consequences, such as serious injuries or impairment of core processes and functions for an extended period of time.

Quantifying Asset Value

After a building's assets requiring protection have been identified, they are assigned a value. The asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets.

FEMA 426 uses a combination of a seven-level linguistic scale and a ten-point numeric scale.

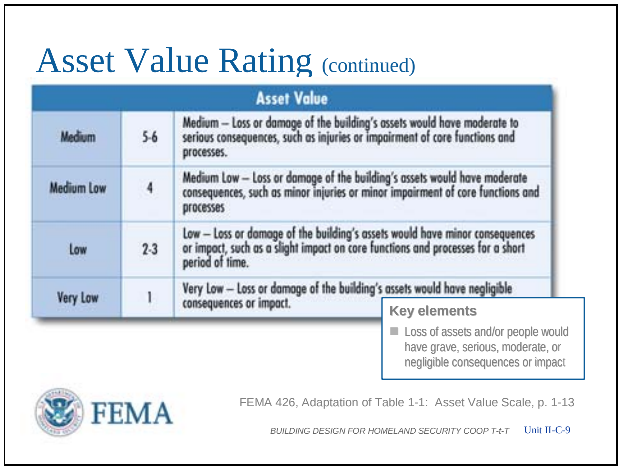
- **Very High –** Loss or damage of the asset would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

loss of primary services, core processes, and functions.

- **High –** Loss or damage of the asset would have grave consequences, such as loss of life, severe injuries, and loss of primary services.
- **Medium High –** Loss or damage of the asset would have serious consequences, such as serious injuries, or impairment of core processes and functions for an extended period of time.

VISUAL II-C-9



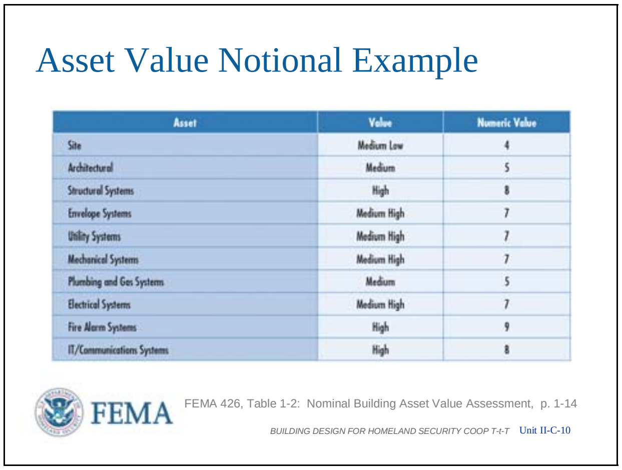
Quantifying Asset Value (continued)

At the other end of the scale we have:

- **Medium –** Loss or damage of the asset would have moderate to serious consequences.
- **Medium Low –** Loss or damage of the asset would have moderate consequences, such as minor injuries, or minor impairment of core functions and processes.
- **Low –** Loss or damage of the asset would have minor consequences or impact.
- **Very Low –** Loss or damage of the asset would have negligible consequences or impact.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL II-C-10



Asset Value Notional Example

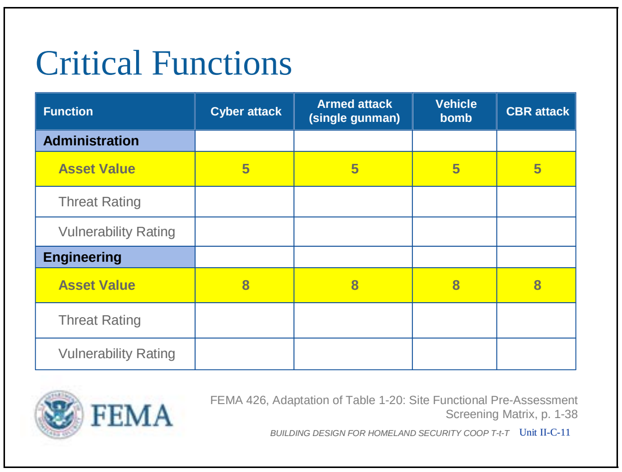
Asset	Value	Numeric Value
Site	Medium Low	4
Architectural	Medium	5
Structural Systems	High	8
Envelope Systems	Medium High	7
Utility Systems	Medium High	7
Mechanical Systems	Medium High	7
Plumbing and Gas Systems	Medium	5
Electrical Systems	Medium High	7
Fire Alarm Systems	High	9
IT/Communications Systems	High	8

Asset Value Notional Example

The key assets for this notional example by system are listed and an asset value rating is entered into the site critical infrastructures matrix.

HVAC mechanical systems in most buildings will likely be medium high (7).

VISUAL II-C-11



Critical Functions

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

Note: The Asset Value under the Administration and Engineering functions is highlighted. A medium value rating (6) is assigned to the Administration function asset value because they are a small part of the total organization, but important to the organization for continuity of business and profit. A high Asset Value rating (8) was assigned for the Engineering Function as they account for over half of the organization and are considered the core of the business for the company.

Critical Functions Matrix

List functions down the left side and threats across the top.

In general, the asset value for a given function is the same for all threats and the matrix helps to identify the primary functions in a quantitative form. The functions matrix is people oriented and is subjective, but the completed matrix should provide a guide to vulnerabilities and risks. An organization with few administrative staff, but with a large engineering group, is used in this example.

Note the value is the same for all threat pairs. It does not matter how the asset is lost. The asset value reflects the impact to the people and organization should the asset be lost, damaged, or degraded.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-C-12

Critical Infrastructure

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

FEMA

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

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit II-C-12

Critical Infrastructure Matrix

List infrastructure down the left side and threats across the top.

Note that the value is the same for all threat pairs to reflect the economic and organization impact losses that could occur over time should the critical infrastructure be lost, degraded, or damaged due to any threat tactic.

Note: The Asset Value rating under the Site and Structural Systems is highlighted. A medium low Asset Value rating (4) could be an initial value for a site infrastructure that has a well-defined and protected perimeter and economic replacement costs that are acceptable. A high Asset Value rating (8) could be an initial value for a Structural System in a multi-story that is subject to progressive collapse and cannot be replaced.

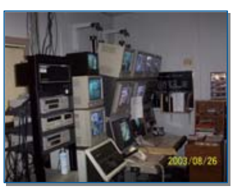
VISUAL II-C-13

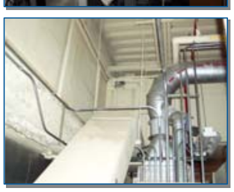
Summary

Identify a building's Critical Functions and Critical Infrastructure

Assign a value to a building's assets or resources

Input values into Critical Functions and Critical Infrastructure areas of Threat Matrix





FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit II-C-13

Summary

- Identify a building's Critical Functions and Critical Infrastructure
- Assign a value to a building's assets or resources
- Insert values into the Critical Functions and the Critical Infrastructure areas of the Threat Matrix
  [Risk Matrix poster, manual spreadsheets, electronic spreadsheets, or risk assessment database]

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-C-14

Asset Value Rating Considerations

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

1. Criticality to overall organization
2. Criticality to unit at location
3. Ease of replacement
4. Relative value ($, # personnel, # critical personnel)
5. Consequences of destruction, failure, or loss of function in terms of casualties, property loss, and economic impacts
6. Likelihood of cascading or subsequent consequences

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit II-C-14

VISUAL II-C-15

Unit II Case Study Activity

Asset Value Ratings

Background

Asset value: degree of debilitating impact that would be caused by the incapacity or destruction of a building's assets

FEMA 426: Tables 1-1 and 1-2

Requirements

Refer to Case Study and answer worksheet questions:

- Identify Core Functions
- Identify Building Assets
- Quantify Asset Values

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit II-C-15

Refer participants to **FEMA 426** and the Unit II Student Activity for the Selected Case Study (C) in the Student Manual.

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

At the end of 35 minutes, reconvene the class and facilitate group reporting.

NOTE to instructor: Work tables and room to draw out student answers, especially when they

Asset Value Rating Considerations

As a further emphasis to ensure understanding of definitions, a review of Asset Value and how it can be looked at is provided here. The list on the slide is expanded with examples on the designated page of the Student Manual.
[It is also the first page of the Case Study Activity later in this document (about 2 pages).]

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

Student Activity

Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of a building's assets.

- **Table 1-1 on Page 1-13 of FEMA 426** provides an **Asset Value Scale** to quantify asset value, as well as definitions of the ratings.
- **Table 1-2 on page 1-14 of FEMA 426** provides a format to summarize the value of the major categories of a building's assets.

Activity Requirements

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

- Working in previously assigned small groups, refer to the Case Study Student Activity (Version C for COOP) and answer the worksheet questions.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**
are different from the "school solution." Point out that team consistency of rationale as applied to all assets is more important than the specific number provided in the rating.	Take 35 minutes to complete this activity. Solutions will be reviewed in plenary group.
Allow 10 minutes for the plenary session.	
Keep in mind that there are no incorrect answers. It is more important to be able to clearly explain and support the underlying rationale for the values that have been assigned. Also it has been proven that 7 people working effectively as a group can achieve genius level in their consensus response.	
	Transition
	Unit III will cover Threat / Hazard Assessment and Unit IV will cover Vulnerability Assessment to continue the risk assessment process.

UNIT II (C) CASE STUDY ACTIVITY:
ASSET VALUE RATING
(COOP Version)

Asset Value Rating Considerations (Impact or Consequences if asset is lost or damaged)

1. Criticality to the overall organization, agency, company, or government entity goals
   - Higher criticality means higher value
     - Number of users affected
     - Direct economic loss and cost to rebuild
     - Potential number of deaths from an attack

2. Criticality to the goals of the specific unit, location, branch, or office being assessed
   - Higher criticality means higher value
     - Number of users affected
     - Direct economic loss and cost to rebuild
     - Potential number of deaths from an attack
   - Example, the loss of the kitchen at a Veterans Affairs Hospital is important to that hospital, but the loss of that kitchen is not critical to the overall goals of the Department of Veterans Affairs.

3. Ease of replacement
   - Harder to replace (measured in months to years) means higher value
   - Easier to replace (measures in days) means lower value

4. Relative value of assets
   - Just like in fire protection assessment, the higher the cost of the items individually and in aggregate, the higher the value
   - For people performing functions, the number of critical personnel and the number of total personnel in the facility determine the relative rating; the higher the number of people the higher the value
   - Critical personnel may be harder to replace due to the time needed for education, training, and experience to meet functional needs; similar to ease of replacement but with much longer timelines

5. What are the consequences of destruction, failure, or loss of function of the asset in terms of fatalities and/ or injuries, property losses, and economic impacts? (Similar to criticality above)
   - Number of users affected
   - Direct economic loss and cost to rebuild
   - Potential number of deaths from an attack

6. What is the likelihood of cascading or subsequent consequences should the asset be destroyed or its function lost?
   - Interdependency – will loss of the asset have an effect upon other assets in the same or different Critical Infrastructure Sectors

UNIT II (C) CASE STUDY ACTIVITY: ASSET VALUE RATING (COOP Version)

Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of a building's assets. **Page 1-13 of FEMA 426** provides an Asset Value Scale **(Table 1-1)** to quantify asset value, as well as definitions of the ratings. **Table 1-2 on page 1-14 of FEMA 426** provides a format to summarize the value of the major categories of a building's assets. **FEMA 452, pages 2-17 to 2-19** provide additional information.

Requirements

Referring to the Appendix C Case Study to determine answers to the following questions:

The first question below has the answer provided as an **example**. The other questions have the pages identified where the answers may be found.

Activity #1: Identifying Building Core Functions

1. What are Cooperville Information / Business Center's (CI/BC) primary services or outputs? [Page C-5 to Page C-6]

   Information Division -- IT services support for over 20 private and government organizations/clients. CI/BC supports over 1,000 users and over 100 applications as a primary data center and as a disaster recovery backup site to include field technicians and help desk. Many clients depend on CI/BC's ability to provide real time IT support, on a 24 x 7 basis. Others rely on the company's IT backup services.

   Business Center – Provides day-to-day office space and office, telephone, and computer support to short-term clients, including Information Division requirements.

2. What critical functions/activities take place at CI/BC? [Page C-31 to Page C-35]

   Computer-based data processing, storage, and disaster recovery. Wired/wireless networking, information technology and communications. Secure office space, conference space, and computer support.

3. Who are the building's occupants and visitors? [Page C-5 to Page C-6]

   CI/BC employees and clients; business park neighbors are a mix of government and commercial organizations. CI/BC has over 75 employees and approximately 25 employees in the building at any given time. Visitors to the Information Division are vendors and clients. Clients include Fortune 500 companies, national and regional banks and credit unions, a major airline,

large prime defense contractors, and government agencies, including one classified client.

The company's business center mission is to provide temporary office support on a short term basis to business travelers or companies who need additional space, including some space at higher security levels. Thus the Business Center can support anyone, but secure space and computer access requires proper verification of security clearance prior to entering any of these spaces.

4. What inputs from external organizations are required for CI/BC's success? [Page C-5 to Page C-6 and Page C-17 to Page C-35]

    Utilities and communications supplies/vendors; hardware and software applications vendors; client data and support. The Business Center relies upon business travelers and existing clients that need temporary office space.

Activity #2: Identifying Building Assets and Quantifying Asset Value Ratings

Use the following process to complete the following tables – CI/BC Critical Functions Asset Value Ratings and CI/BC Critical Infrastructure Asset Value Ratings.

<u>Adjust your asset value ratings</u> of CI/BC's critical functions and critical infrastructure <u>based upon the COOP needs of DAI</u>.

1. Refer to **Table 1-1 in FEMA 426** and the associated value descriptions for the ratings listed below
    - Very High (10)
    - High (8-9)
    - Medium High (7)
    - Medium (5-6)
    - Medium Low (4)
    - Low (2-3)
    - Very Low (1)

2. Consider the questions on **page 1-11 in FEMA 426** as you rate CI/BC's assets.

3. Refer to **Table 1-2 in FEMA 426, Nominal Building Asset Value Assessment** and use the descriptions of these asset categories as found in the Appendix C Case Study to focus the rating. <u>Another approach</u> is to use an asset value rating of 5 (mid-range) and do a pair-wise comparison to each asset category as the process continues, raising or lowering the rating from 5 as the team compares asset value inputs collected from the Appendix C Case Study.

NOTE 1: The first two rows in both tables are completed as **examples**. Nominal ratings are provided in all other asset categories.

1. Confirm the team's Asset Value Rating for each category [agree, raise, or lower the indicated rating]
2. Provide Rationale for each rating [whether changed or unchanged]
3. Enter asset value rating on the Risk Matrix

NOTE 2: Consult **Table 1-22, pages 1-46 to 1-92, in FEMA 426.** Look at the content of the questions to understand the various infrastructure asset categories.
For example, Utility Systems apply to all utilities outside the 3-foot drip line of the building (from the source to the building, but primarily on the site), while Mechanical, Plumbing, Gas, Electrical, Fire Alarm, Communications, and Information Technology Systems are inside the 3-foot drip line of the building.

CI/BC Critical Functions Asset Value Ratings

Asset	Value	Numeric Value	Rationale
1. Administration	Medium-Low	4	Redundancy and staff skills that can be replaced. Senior managers and financial systems in the same area increase value. Low to medium economic cost to replace. Can impair in the short term the core functions and processes. DAI COOP value is minimal as ERG is self-contained, at least for the first 30 days.
2. Engineering / IT Technicians	High	8	Staff skills require specialized expertise, but can be replaced. Key equipment and resources needed for 24/7 ops. High economic cost to replace. Can impact core functions and processes for extended period of time. DAI COOP value is high as this function ensures connectivity and communications.
3. Loading Dock / Warehouse	Medium-Low	4	***Single point of entry into the interior for major shipping and receiving. Low to medium economic cost to replace. Can use other entryways in interim for most items. Minor impairment of core functions and processes. DAI COOP value is no different from CI/BC.***
4. Data Center	Very High	10	***Primary function and organization critical. Many key staff and critical equipment. Very high economic cost to replace. Vital for 24/7 operation. Total loss of primary services, core***

Asset	Value	Numeric Value	Rationale
			processes, and functions possible. DAI COOP value is equivalent to CI/BC.
5. Communications	High	9	***Primary function and organization critical. A few key staff and critical equipment. High economic cost to replace. Needed for 24/7 operation. Major affect on primary services and core functions and processes for extended period of time. DAI COOP value is equivalent to CI/BC.***
6. Security	Medium High	7	***Access and monitoring systems, security records, and location make the function critical to the organization. Needed due to client requirements. Medium economic cost to replace. Serious impairment of primary services, core processes and functions for extended period of time. Security is also necessary for the Business Center, especially the controlling of access to secure space and the identification of Business Center users. The latter need may increase the asset value rating. DAI COOP value may be higher than CI/BC due to ERG personnel and essential functions on site.***
7. Housekeeping	Very Low	1	***Easily replaced, no critical skills or equipment. Minimal cost to replace. Many workarounds, thus negligible consequences or impact. DAI COOP value is equivalent to CI/BC.***

CI/BC Critical Infrastructure Asset Value Ratings

Asset	Value	Numeric Value	Rationale
1. Site	Medium-Low	4	CI/BC does not own building or site, but location is critical to access and support to clients. Cost is \$10 - \$20 per square

Asset	Value	Numeric Value	Rationale
			foot which indicates other office complexes in area are competitive. Moderate consequences or minor impairment of core processes and functions if must move from site. DAI COOP value can be higher than CI/BC, due to CI/BC backup of DAI data.
2. Architectural	Medium	5	Signage and business office information couple the building to other park tenants (geographically clustered, centralized). Nothing overly descriptive that requires the use of this building, but moderate to severe consequences or impairment if lost. Limited architectural flexibility either exterior or interior. DAI COOP value no different than CI/BC, as long as signage remains non-descript. Building layout will be as is.
3. Structural Systems	Medium-Low	8	***Relatively strong and flexible two-story building using standard construction will not experience progressive collapse, but has a great potential for localized collapse. Loss of structural systems in whole or in part would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core functions and processes for an extended period of time. DAI COOP value equivalent to CI/BC.***
4. Envelope Systems	Medium	5	***Fairly tight envelope, newer construction, CBR agents not likely to penetrate into interior through wall cracks or roof gaps without longer contact time. Over 50 percent of exterior surface is glazing on front and one-third of the side where glazing exists. Loss of any envelope system will have moderate to serious consequences or impairment of core functions and processes mainly due to environmental effects—weather entering building. A higher rating may***

Asset	Value	Numeric Value	Rationale
			be in order based upon security requirements. DAI COOP value may justify higher value also based upon security needs.
5. Utility Systems	Medium	5	***Necessary for efficient and economic operation. Commercial utilities have high reliability in area. Loss of one or more utility systems would have moderate to serious consequences and impairment of core functions and processes. Backups in-place indicate the recognized value of these systems. DAI COOP value equivalent to CI/BC.***
6. Mechanical Systems	High	8	***Single HVAC system supports multiple HVAC Air Handling Units and interior spaces. High economic cost to replace. Loss of business revenue. Limited workarounds due to location of HVAC load within building. Loss of HVAC and chilled water seriously hampers core functions and processes. DAI COOP value equivalent to CI/BC.***
7. Plumbing and Gas Systems	Medium	6	***Wet pipe sprinkler system and hand-held extinguishers are means of fire protection in this 24/7 operation. Natural gas provides some humidity control for core processes but workarounds (portable dehumidifiers) possible. Water for cooling tower makeup is critical to support core processes, but workaround (water tanker) possible. Moderate to serious consequences or impairment of core functions and processes if lost. DAI COOP value equivalent to CI/BC.***
8. Electrical Systems	High	8	***Grave consequences to loss of this primary service. High economic cost to replace, but more so loss of business revenue if systems cannot operate. Commercial utility with backup***

Asset	Value	Numeric Value	Rationale
			generator required to meet 24/7 requirements. DAI COOP value equivalent to CI/BC.
9. Fire Alarm Systems	Medium	5	***Wet pipe sprinkler system and hand-held extinguishers are only means of fire protection. Fire alarm system provides additional coverage – heat and smoke detectors. Nearby fire department has connection to alarm. Moderate to serious consequences or impairment of core functions or processes if lost. Workarounds (roving fire watchmen) possible. DAI COOP value equivalent to CI/BC.***
10. IT / Communications Systems	High	9	***Single-point vulnerability and organization critical. High economic cost to replace, <u>but replaceable</u>. Loss of business revenue. Loss of primary services or major loss of core processes and functions for an extended period. DAI COOP value may be higher than CI/BC due to greater communications needed.***

This page intentionally left blank

Unit III (C)

COURSE TITLE

Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer

TIME 75 minutes

UNIT TITLE

Threat/Hazard Assessment

OBJECTIVES

1. Identify the threats and hazards that may impact a building or site.
2. Define each threat and hazard using the 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.

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 FEMA 426 approach to determine threat rating.
4. A rating scale and how to use it to determine a threat rating.
5. 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 and provide the rationale for these threat ratings.

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 C: COOP, Cooperville Information / Business Center
4. Student Manual, Unit III (C) (info only – not in SM)
5. Unit III (C) 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 (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit III (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

UNIT III (C) OUTLINE

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.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The 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 (Unit #) 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, all instructors should closely observe the groups' process and progress. If any groups are struggling, immediately assist them by clarifying the assignment and providing as much help as is necessary for the groups to complete the requirement in the allotted time. Also, monitor each group for full participation of all members. For example, ask any student who is not fully engaged a question that requires his/her viewpoint to be presented to the group.
- At the end of the working period, reconvene the class.
- After the students have completed the assignment, "walk through" the activity with the students during the plenary session. Call on different teams to provide the answer(s) for each question. Then simply ask if anyone disagrees. If the answer is correct and no one disagrees, state that the answer is correct and move on to the next requirement. If there is disagreement, allow some discussion of rationale, provide the "school solution," and move on.
- If time is short, simply provide the "school solution" and ask for questions. Do not end the activity without ensuring that students know if their answers are correct or at least on the right track.
- Ask for and answer questions.

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

(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

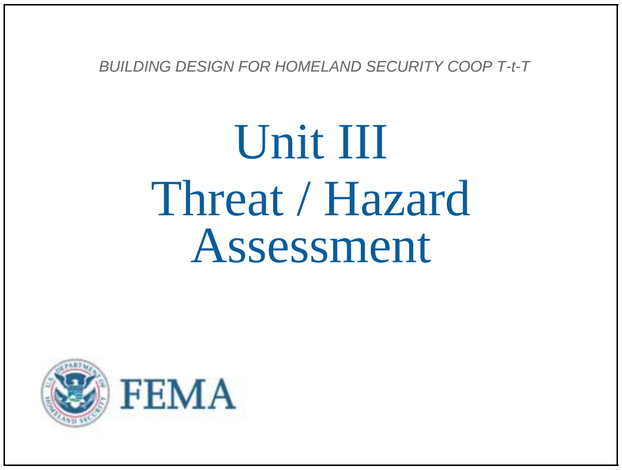
(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-1



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 seven components used to define a threat (or hazard) is adapted 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-C-2

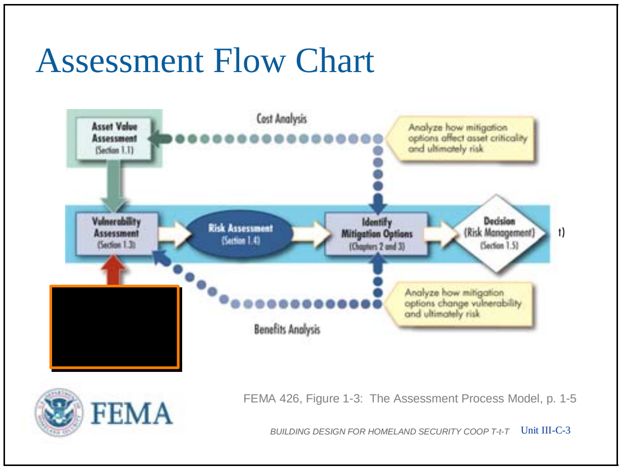
Unit Objectives

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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

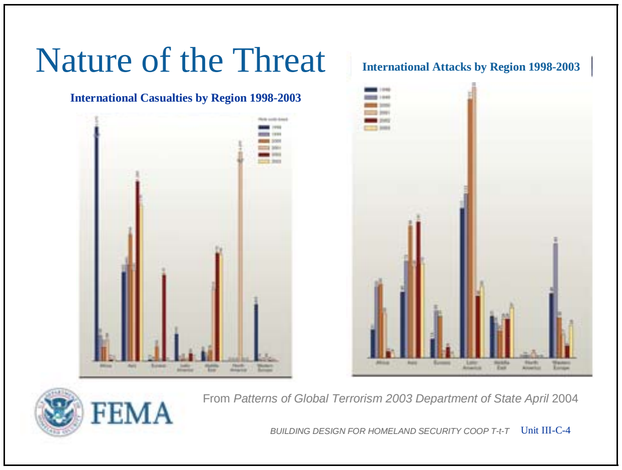
VISUAL III-C-3



Assessment Flow Chart

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

VISUAL III-C-4



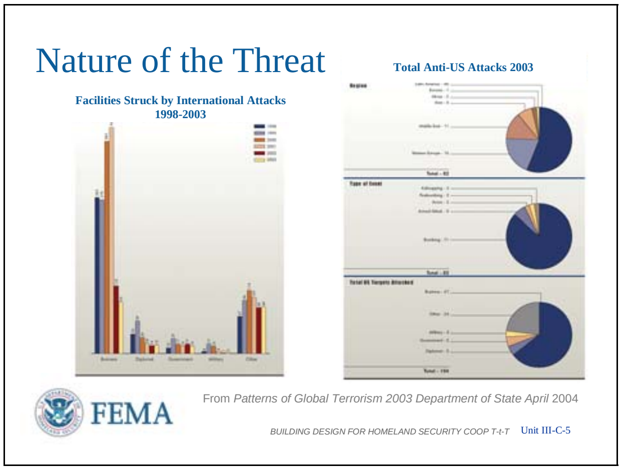
Nature of the Threat (1/3)

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.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL III-C-5	**Nature of the Threat (2/3)**

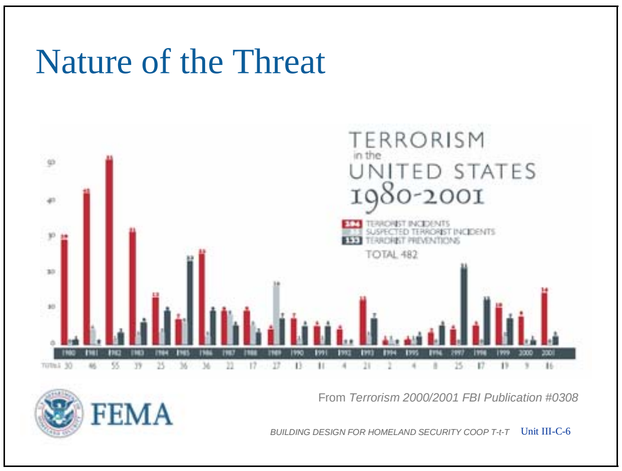


This slide illustrates Anti-US attacks are predominantly NOT against diplomatic, government, and military targets, but against <u>business and others</u>.

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

VISUAL III-C-6

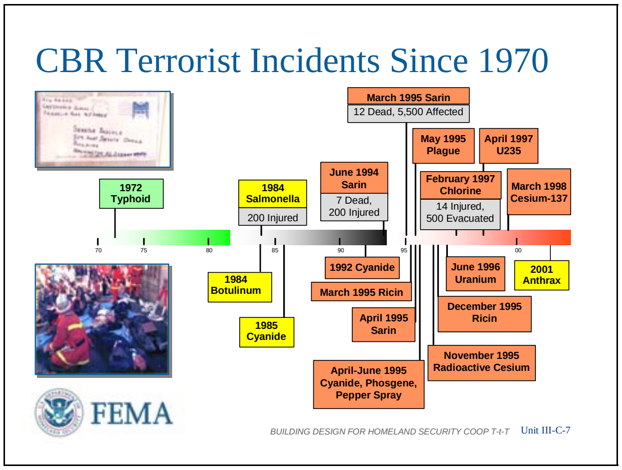
Nature of the Threat (3/3)



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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-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-C-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*).
- <u>The risks of natural hazards may be increased or decreased as a result of human activity</u>. (Like building in a floodplain (bad) or hardening for hurricanes (good))

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-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-C-10

Two-Step Process

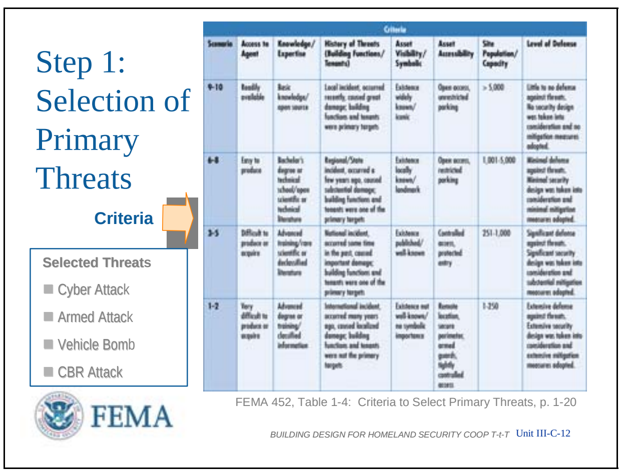
A two-step process is utilized to complete the threat assessment.

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

INSTRUCTOR NOTES

VISUAL III-C-11

VISUAL III-C-12



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

NOTE: Step 1 obscures the true meaning of threat by incorporating in this slide items that are assets and vulnerabilities (which a terrorist may use to determine the suitability of a building as a target.

In the DoD perspective, **threat** (potential threat elements—people with bad intentions) is based upon:

1. Existence

CONTENT/ACTIVITY

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.

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).

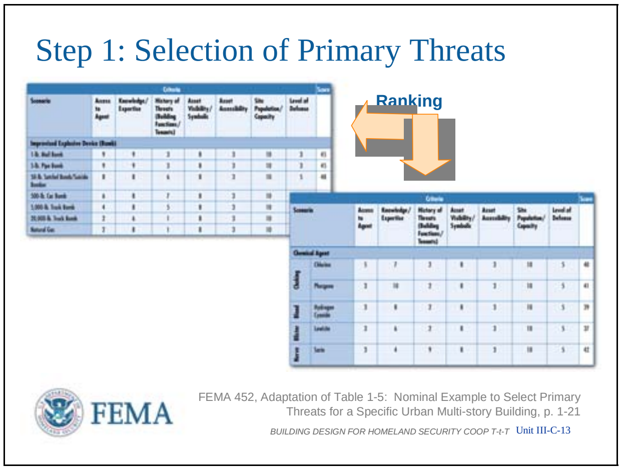
- **Access to Agent:** The access to agent is the ease by which the source material can be acquired to carry out the attack. Consideration includes the local HazMat inventory, farm and mining supplies, major chemical or manufacturing plants, university and commercial laboratories, and transportation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

INSTRUCTOR NOTES	CONTENT/ACTIVITY
2. **Capability** [Access to Agent; Knowledge / Expertise] **3. History** [History of Threats Against Buildings] **4. Intentions** **5. Targeting** All the above concentrate upon the existence and actions of the people who are considered the threat. Comparison to the criteria in this slide is included in the brackets above or listed below: ▪ Asset Visibility/Symbolic – ASSET VALUE. This may link with Intentions (written or spoken) and Targeting (actual surveillance of structure), but in and of itself is a measure of asset value. ▪ Asset Accessibility – VULNERABILITY. This may link with Targeting (actual surveillance of structure), but in and of itself is identification of a weakness to an attack tactic and a measure of vulnerability. ▪ Site Population/Capacity: Same comment as for Asset Visibility/Symbolic above, ▪ Level of Defense: Same comment as for Asset Accessibility above.	• **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?

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-13

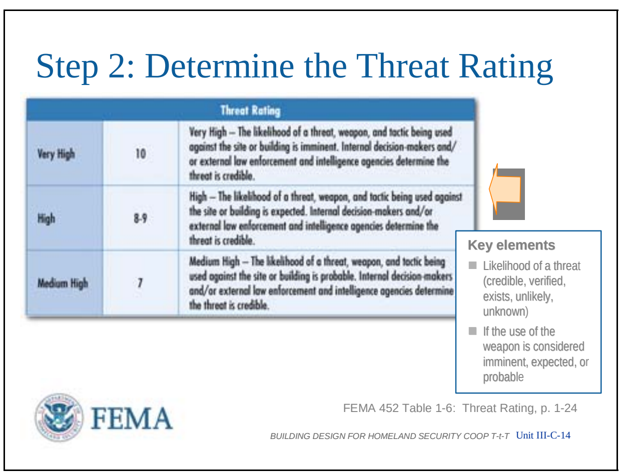


Selection of Primary Threats

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-C-14



Step 2: Determine the Threat Rating

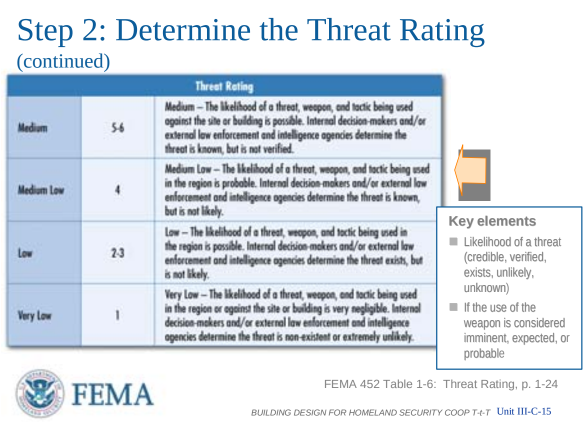
Having selected the primary threats for the building, the next step is to determine how the threat will affect the functions and critical infrastructure. The threat rating is an integral part of the risk assessment and is used to determine, characterize, and quantify a loss caused by an aggressor using 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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

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-C-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.

INSTRUCTOR NOTES

VISUAL III-C-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

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

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit III-C-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 of the assets against 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.

CONTENT/ACTIVITY

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 using some consistent criteria, like DoD's or FEMA's or Federal Marshal Service's (basis of GSA approach).

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) as a starting point. The threat against each asset can then be refined based upon available information. 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.

INSTRUCTOR NOTES

VISUAL III-C-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

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

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit III-C-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 active seismic dampers. The seismic dampers could be part of a “smart building” system where the responsive dampers are adjusted for the accelerations imposed upon the structure, especially high-rises.

CONTENT/ACTIVITY

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.

NOTE to instructor: The ratings on this slide are right out of the example in FEMA 426. It is unrealistic to assume that Structural Systems would get a threat rating of 3 under Cyber Attack and the same rating of 3 under vehicle attack. When updating FEMA 426 the goal will be to decrease the Cyber Attack threat on Structural Systems (to 1) and increase the Vehicle Bomb threat on this same system (to 8).

INSTRUCTOR NOTES

VISUAL III-C-18

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.

CONTENT/ACTIVITY

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:

- Southern Poverty Law Center tracks hate groups in the United States at their web site: www.splcenter.org
- IntelCenter tracks world terrorist groups and has statistics on many aspects of their operations at their web site: www.intelcenter.com

INSTRUCTOR NOTES

VISUAL III-C-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.

CONTENT/ACTIVITY

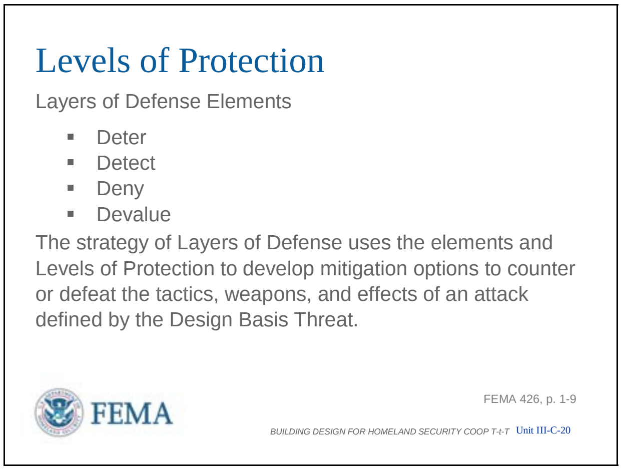
Design Basis Threat

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."

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-20



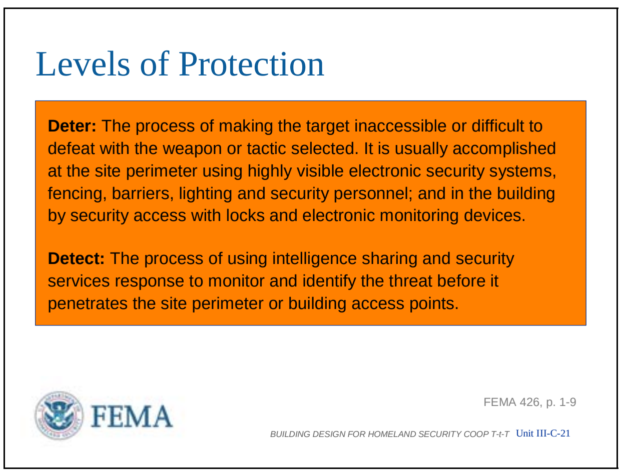
Levels of Protection (1/3)

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

- <u>Deter</u>
- <u>Detect</u>
- <u>Deny</u>
- <u>Devalue</u>

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

VISUAL III-C-21



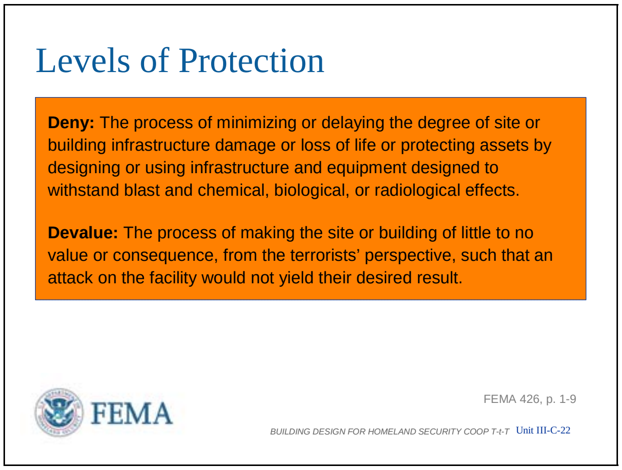
Levels of Protection (2/3)

Layers of Defense elements

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-22

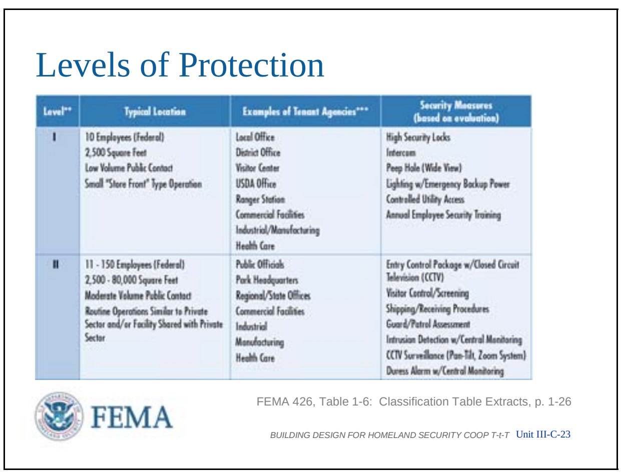


Levels of Protection (3/3)

Layers of Defense elements

- Deny
  - o 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.
  - o Hardening the asset so as to withstand the employment of the tactic without detriment to people, critical functions, or critical infrastructure
- Devalue
  - o Make the asset a less desirable actual or perceived target by dispersing, camouflage, concealment, or deception

VISUAL III-C-23



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

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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-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 COOP T-t-T Unit III-C-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-C-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 COOP T-t-T Unit III-C-25

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

NOTE to instructor: The DoD standard shown here as contained in FEMA 426 is dated 31 July 2002. The most recent version of this standard is dated 22 January 2007 and has different descriptions of damage and injury for each Level of Protection. The most recent standard can be found on the Student Reference CD.

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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-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 COOP T-t-T Unit III-C-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-C-27

Levels of Protection

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

FEMA

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

Levels of Protection (1 of 2)

DoD Antiterrorism Standards 1 to 12.

NOTE to instructor: These DoD standards have been updated to the 22 January 2007 version.

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

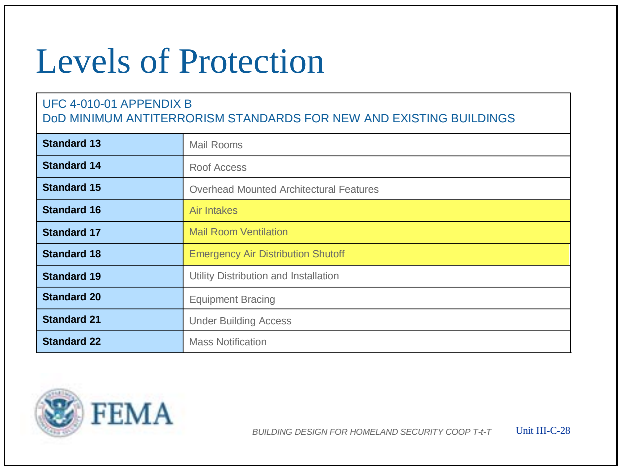
- DOD Std 1 – Standoff Distances
  - Separation distance – vehicle bomb to building
  - Analysis to show level of protection achieved if minimum stand-off cannot be met
- DoD Std 2 – Unobstructed Space
  - Clear Zone around building preventing a package bomb from being hidden
  - No equipment or enclosures within unobstructed space
- DoD Std 4 – Access Roads
  - Access control measures that ensure unauthorized vehicles do not get inside the minimum stand-off

INSTRUCTOR NOTES	CONTENT/ACTIVITY

distance

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

VISUAL III-C-28



Levels of Protection (2 of 2)

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 – Mail Room 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 into 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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-C-29

Summary

The process for developing threat assessments:

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

Use Federal, state, or local law enforcement and other government functions to help determine threat ratings.

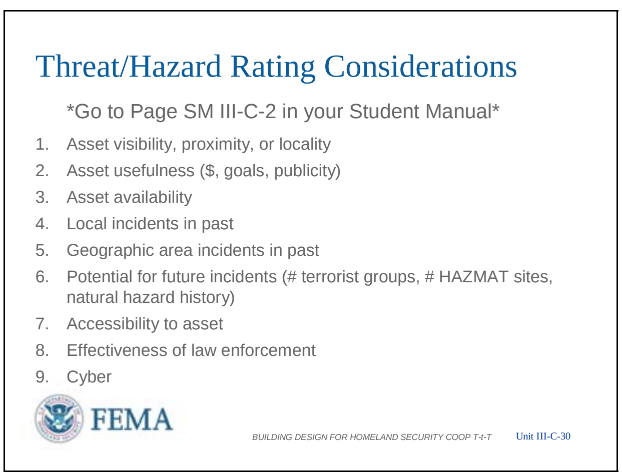
Complete the Critical Functions and Critical Infrastructure Matrices.

Establish the Design Basis Threat.

Select the Level of Protection.

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

VISUAL III-C-30



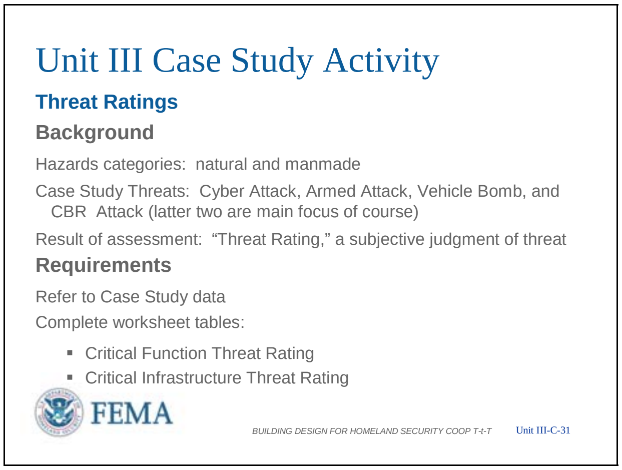
Threat / Hazard Rating Considerations

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

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

INSTRUCTOR NOTES

VISUAL III-C-31



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.

At the end of 30 minutes, reconvene the class.

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

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

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

CONTENT/ACTIVITY

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 can be categorized into two groups:

- Natural
- Manmade – Technological Accidents or Terrorist Initiated

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"

- The result of this assessment is a "Threat Rating."

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

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

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- CI/BC Critical Functions
- CI/BC 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.

UNIT III (C) CASE STUDY ACTIVITY: THREAT/HAZARD RATING (COOP Version)

Threat/Hazard Rating Considerations (Likelihood of Attack or Occurrence)

1. Asset visibility to terrorists, proximity to technological hazards, or locality for natural hazard
   - Higher visibility, closer proximity to technological hazards, or location within specific locality for natural hazards raise threat rating
     - Iconic structure is considered highest visibility
   - Lower visibility, far from technological hazards, and not located where earthquake, wind, fire, or flood are known dangers would lower threat rating
   - List from FEMA 386-2 as potential hazards
     - Avalanche
     - Coastal Erosion
     - Coastal Storm
     - Dam Failure
     - Drought
     - Earthquake
     - Expansive Soils
     - Extreme Heat
     - Flood
     - Hailstorm
     - Hurricane
     - Land Subsidence
     - Landslide
     - Severe Winter Storm / Ice Storms, Heavy Snows, Transportation restricted
     - Tornado
     - Tsunami
     - Volcano
     - Wildfire
     - Windstorm
     - Added: Extended loss of water, sewage, or electric utilities
     - Added: Extended loss of garbage or debris collection

2. Usefulness of assets with cash value, with direct application to attacker's goals, or with publicity value
   - Generally, higher the cash value, greater applicability to terrorist goals, and great publicity value, the higher the threat from criminals and terrorists and the higher the rating

3. Asset availability
   - If available at one location only – high threat rating)
   - If available everywhere – low threat rating

4. Number of local incidents in the past
    - The higher the number of incidents (all potential sources) the higher the threat rating

5. Number of incidents in the geographic area in the past
    - The higher the number of incidents (all potential sources) the higher the threat rating

6. Potential for future incidents -- subjective view of likelihood that can be adjusted for the following:
    - The higher the number of terrorist organizations operating with ability or desire to be in the vicinity the higher the threat rating
    - The higher the number of potential technological hazards sites nearby the higher the threat rating
    - The expected future occurrence of flood, wind, and seismic activity in the specific locality the higher the threat / hazard rating

7. Accessibility to asset (this is used as a threat input by many methodologies, but could be viewed as a vulnerability consideration as explained below)
    - The fewer layers of defense in place, the higher the threat rating – This is based upon the terrorist assessment of the building as a future successful target
    - DETER and DETECT measures as defined on page 1-9 of FEMA 426 are methods for reducing the threat
    - DENY measures as defined on page 1-9 of FEMA 426 are methods of hardening the site and building and would be described better as mitigation of vulnerability

8. Effectiveness of law enforcement (including counter intelligence)
    - Greater the effectiveness, the lower the threat rating – Detect

9. Cyber
    - Does function or infrastructure have any components using electronics, software, or data (information technology) or communications
        - If yes, then threat is high due to the ease of identifying / pinging these systems
        - If no, then threat is low
        - Level of threat is relative to the value of information contained or the consequences of change that would draw the terrorist or hacker to want to enter the system
    - Cyber experts go into much greater detail, but essentially are looking at a common vulnerability standard vice a threat rating

UNIT III (C) CASE STUDY ACTIVITY: THREAT/HAZARD RATING (COOP 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 C Case Study data and complete the following worksheets. Each student as part of their assessment team will interpret the CI/BC threat information and should select and justify a threat/hazard rating number with rationale.
For example:

- 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 Activity # 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.

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

- Activity # 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.

- Activity # 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 Activity # 2 Threat Ratings tables below to the Risk Matrix poster after team agreement on answer.

Activity # 1: Determine the threat score for a 500-lb. vehicle bomb as applied to CI/BC

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 C Case Study.

As shown in Table 1-5, page 1-22, FEMA 452, (and provided on page ***IG III-C-25*** of this unit, ***SM III-C-5*** of Student Manual Unit III) 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 a target)
- Asset Accessibility (Vulnerability)
- Site Population / Capacity (Asset Value or Threat (Targeting))
- Level of Defense (Vulnerability)

FEMA 452 Table 1-4 Criteria								
Scenario	Access to Agent	Knowledge/ Expertise	History of Threats Against Buildings	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense	Score
Improvised Explosive Device (Bomb)								
500 lb. Vehicle Bomb	***9***	***9***	***6***	***4***	***10***	***2***	***10***	***50***

Rationale for Above Numbers using FEMA 452 Criteria on next page

- ***Access to Agent -- Readily available – "Farm" explosives but with some restrictions***
- ***Knowledge/Expertise --Instructions on internet***
- ***History gets a higher rating closer to home -- Regional/State low end good choice for suburban environment with nearby metropolitan area and military installations***
- ***Asset Visibility / Symbolic– Existence published***
- ***Asset Accessibility – open access, unrestricted parking***
- ***Site Population – less than 250***
- ***Level of Defense – Little or no defense against threats. No specific security design taken into consideration or adopted for this threat.***

FEMA 452 Criteria

Scenario	Access to Agent	Knowledge/ Expertise	History of Threats Against Buildings	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense
9-10	Readily available	Basic knowledge/ open source	Local incident	Existence widely known/ iconic	Open access, unrestricted parking	> 5,000	Little or no defense against threats. No security design was taken into consideration and no mitigation measures adopted.
6-8	Easily producible	Bachelor or technical school/open scientific or technical literature	Regional/ State	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	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	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.

Activity # 2: Determine the Threat Ratings for Cooperville Information / Business Center

This 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, no intent.

> Recommendation: For Cyber Attack against an asset that has no computer and no connection to the internet the Threat Rating should be based upon the asset having a computer internet connection. Then handle the lack of computer and/or lack of internet connection under the Vulnerability Rating. Then if the asset gets a future computer and/or future internet connection only the Vulnerability Rating need be adjusted.

NOTE 3: In the Critical Functions and Critical Infrastructure Threat Ratings below, Armed Attack has threat ratings and rationale completed as an example. Review Armed Attack and adjust as the team sees fit and then complete the remainder of the Threat Ratings tables.

CI/BC Critical Functions Threat Ratings

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

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
Rationale	***8 -- High threat of cyber attack upon any system with access through internet, landline communications, or wireless communications due to history and targeting.*** ***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 would increase threat rating by increasing accessibility.***	3 -- Low threat based upon lack of intentions, history, or targeting in the locale, region, state, and nation. Criminal activity notwithstanding is normally focused on more transient sites with easy get-away access.	***6 -- Medium threat due to national and international groups with capability, intentions, history, and targeting expertise.*** ***However, no local, regional, or state experience.***	***4 – Medium-low threat due to international groups with capability, intentions, and history.*** ***Local groups with history and targeting have been more focused in their tactics and not on a building-wide basis.***

CI/BC Critical Infrastructure Threat Ratings

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

Infrastructure	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
Rationale	***1 or 2 -- Very Low or Low threat of cyber attack due to lack of history and targeting upon this infrastructure with little benefit to support intentions.*** ***5 -- Medium threat due to lack of history and targeting upon this building infrastructure, but increased benefit to support intentions if more than one building can be involved.*** ***10-- Very High threat of cyber attack due to past history of intent and targeting of IT / Communications Systems for criminal, terrorist, or intelligence (commercial or national) gain.***	3 -- Low threat based upon lack of intentions, history, or targeting of infrastructure on the local, regional, state, and national levels. 5 -- Medium threat on certain infrastructure systems (normally found outside the building envelope) that have been targeted and impacted by armed attack.	***6 -- Medium threat due to national and international groups with capability, intentions, history, and targeting expertise.*** ***However, no local, regional, or state experience.*** ***Infrastructure directly targeted due to media value of resultant building damage and resultant casualties.***	***4 -- Medium Low threat due to international groups with capability, intentions, and history.*** ***Local groups with history and targeting have been more focused in their tactics and not on a building-wide basis.*** ***Infrastructure <u>not</u> directly targeted but impacted by collateral damage.***

Unit IV (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 105 minutes
UNIT TITLE	Vulnerability Assessment
OBJECTIVES	1. Explain what constitutes a vulnerability. 2. Identify vulnerabilities using the Building Vulnerability Assessment Checklist. 3. Understand that an identified vulnerability may indicate that an asset is vulnerable to more than one threat or hazard and that mitigation measures may reduce vulnerability to one or more threats or hazards. 4. Provide a numerical rating for the vulnerability and justify the basis for the rating.
SCOPE	The following topics will be covered in this unit: 1. Review types of vulnerabilities, especially single-point vulnerabilities and tactics possible under threats/hazards for which there are no mitigation measures. 2. Various approaches and considerations to determine vulnerabilities – FEMA (primarily), with inputs from Departments of Defense, Justice, and Veterans Affairs. 3. A rating scale and how to use it to determine a vulnerability rating. 4. Activity: Determine the vulnerability rating, with rationale, for each asset-threat/hazard pair of interest, using the four threats selected for this course (Cyber Attack, Armed Attack, Vehicle Bomb, CBR Attack) as applied against the identified assets. Achieve team concurrence on answers.
REFERENCES	1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-24 to 1-35 and pages 1-45 to 1-93 2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-1 to 3-20 3. Case Study – Appendix C: COOP, Cooperville Information / Business Center 4. Student Manual, Unit IV (C) (info only – not listed in SM) 5. Unit IV (C) visuals (info only – not listed 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 IV (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit IV (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

UNIT IV (C) OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** This is a generic instruction unit, but it has great capability for linking to the Local Area. Local Area discussion may be generated as students have specific situations for which they would like to determine vulnerabilities or vulnerability rating prompted by points brought up in the presentation.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will apply the vulnerability identification (or lack of mitigation measures) and vulnerability rating to the Case Study to identify and rate the vulnerabilities found in the Case Study for each asset-threat/hazard pair of interest. The students will quickly review/scan the building data, physical security, building structure, electrical systems, mechanical systems, information systems, communications, emergency response, and geographic information system (GIS) portfolio to have a sense of the vulnerabilities at the building being assessed. The **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)** can be used to capture the sense of potential vulnerabilities and mitigation measures.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page (Unit #) in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- Explain that the vulnerability ratings determined by the team must be transferred to the Risk Matrix poster.

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

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

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

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

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

- Ask for and answer questions.

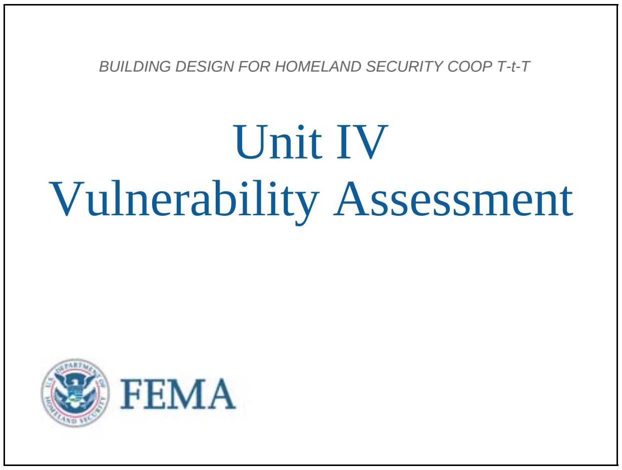
Editor Note: Two methods have been used in Instructor Guides to ensure the slide designation and slide thumbnail in the left column aligns with the Content/Activity in the right column.

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

This page intentionally left blank

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL IV-C-1

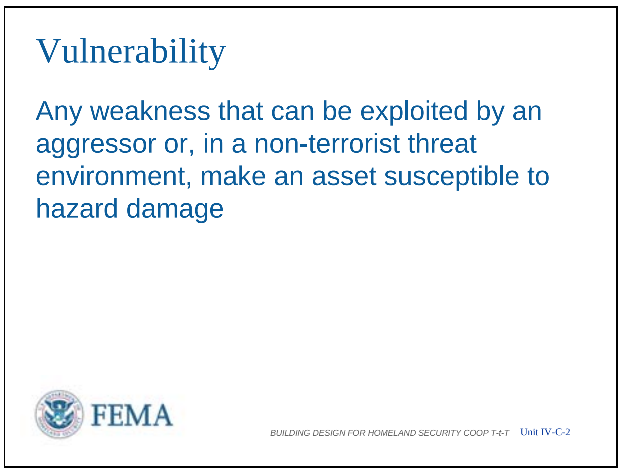


Introduction and Unit Overview

This is Unit IV Vulnerability Assessment. In this unit, we will review types of vulnerabilities, considerations to identifying vulnerabilities, and review a vulnerability rating scale.

This unit also introduces the **FEMA 426 Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93)** to assist in identifying vulnerabilities. This checklist will see extensive use in Units IX, X, and XI (9, 10, and 11).

VISUAL IV-C-2



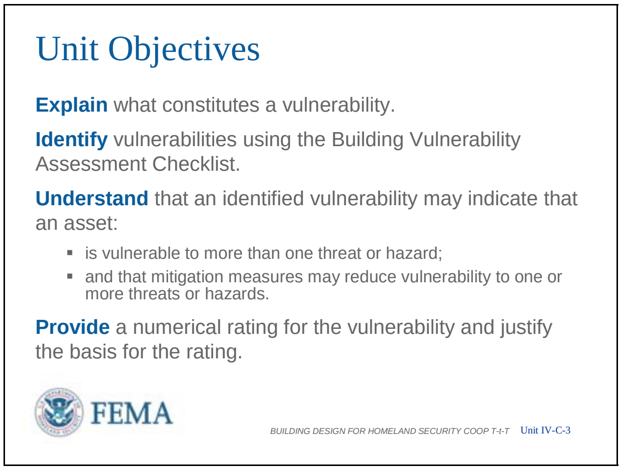
Vulnerability

The definition of vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage.

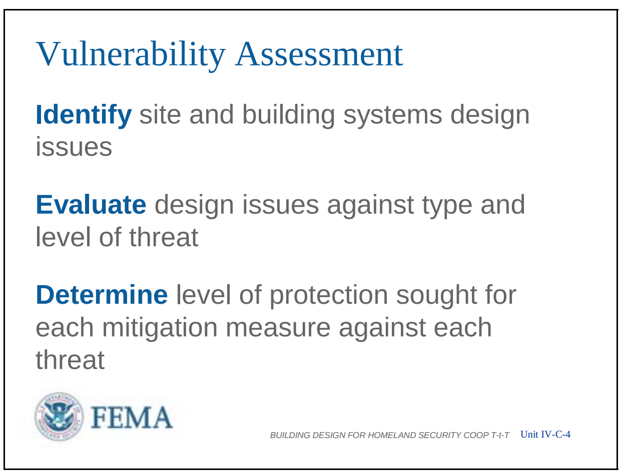
Essentially it is looking at a tactic against an asset and how successful that tactic can be.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-3



VISUAL IV-C-4



Unit Objectives

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

1. Explain what constitutes a vulnerability.

2. Identify vulnerabilities using the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)**.

3. Understand that an identified vulnerability may indicate that an asset is vulnerable to more than one threat or hazard, and that mitigation measures may reduce vulnerability to one or more threats or hazards.

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

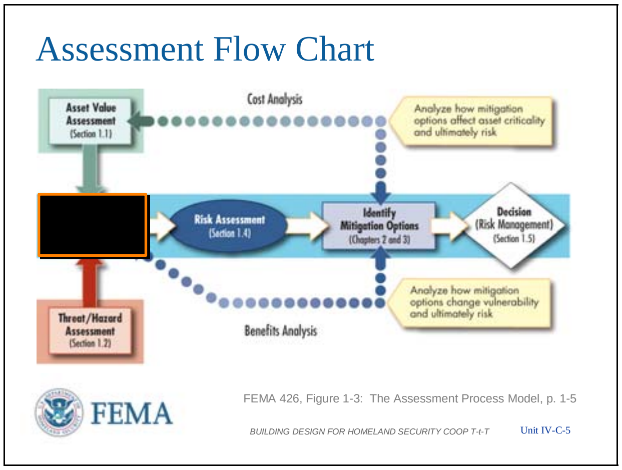
Vulnerability Assessment in this context has three components:
- Identify site and building systems design issues
- Evaluate design issues against type and level of threat
- Determine level of protection sought for each mitigation measure against each threat

[The goal is to see if existing conditions provide the level of protection desired. Then mitigation measures are sought to achieve the level of protection where it has not been achieved.]

Vulnerability assessments occur at different levels or magnitude of scale, including:
- State / Regional / Business Sector
- Site / Building / Tenant or Occupant

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-5



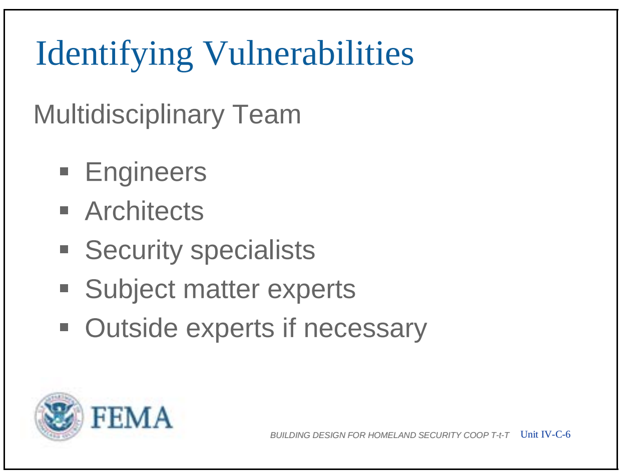
Assessment Flow Chart

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

In the prior steps, assets and their respective values were assigned, the threat was analyzed, a Design Basis Threat was established, and a Level of Protection was selected.

The next step is to conduct the vulnerability assessment, which is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities.

VISUAL IV-C-6



Identifying Vulnerabilities

Assessing a building's vulnerabilities requires a multidisciplinary team. It should not be conducted solely by an engineer or by a security specialist. Only a balanced team can have an understanding of the identified aggressors or threat/hazards and how they can affect the building's critical functions and infrastructure.

Team members include:

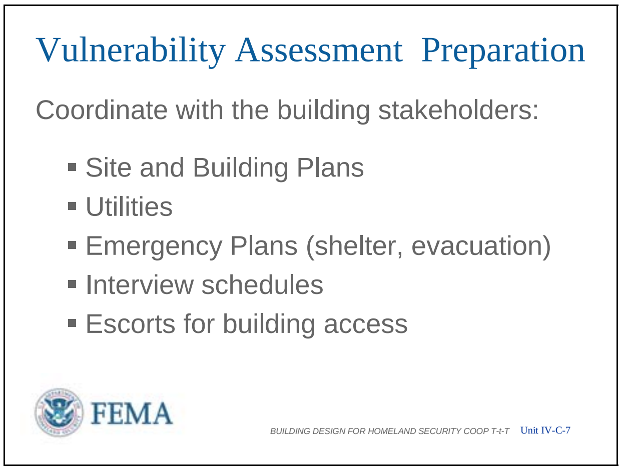
- Engineers
- Architects
- Security specialists
- Subject matter experts
- Outside experts if necessary

Tailor the team to the individual project. A building owner could use his handyman, the local sheriff, his workers, the local volunteer fire department, the service representatives from the local utilities, etc., for an initial

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

assessment. What cannot be answered by this initial team can then be taken to personnel at the next higher level(s) with more expertise and experience in the respective areas.

VISUAL IV-C-7



Vulnerability Assessment Preparation

After assembling a team, the assessment process starts with a detailed planning and information collection of the site. If possible, the information should be gathered in a GIS format.

Types of coordination with the building stakeholders include:

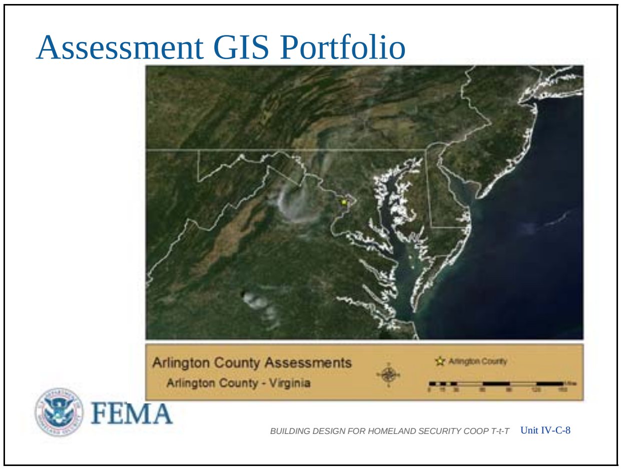
- Site and Building Plans
- Utilities
- Emergency Plans (shelter, evacuation)
- Interview schedules [ensure the people who can answer the team assessment questions are available]
- Escorts for building access

Note that no matter how much preparation is done prior to an assessment, the process on site will reveal new information. Conversely, if preparation is not done, much can be missed because the “right” questions may not have been asked on site.

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

INSTRUCTOR NOTES

VISUAL IV-C-8



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

Another important resource out of the Geospatial One-Stop initiative is www.geodata.gov, a one-stop source of geospatial information from across the nation. Geospatial information allows decisions to be viewed in a community context (e.g., showing the geographic components of buildings, lifelines, hazards, etc.).

Google Earth is also a powerful tool for the novice to gather like information.

CONTENT/ACTIVITY

Assessment GIS Portfolio

A technique to organize required information is to develop an Assessment GIS Portfolio. The portfolio is designed to support vulnerability and risk assessments through identification of:

- Critical infrastructure
- Critical nodes within the surrounding area.
- Nearby functions, including emergency response

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

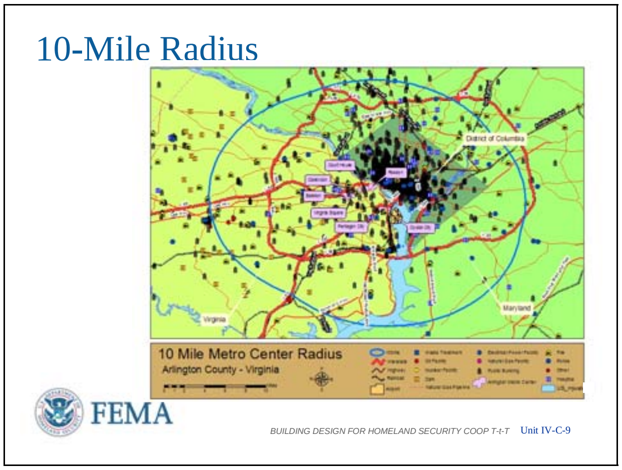
Portfolios are tailored to each individual site.

This slide displays a satellite image of the region with state boundaries delineated. This map provides a general overview for user's initial orientation to a site.

The next series of slides shows how GIS can be used in an outside-to-inside approach to support threat analysis and vulnerability assessments.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

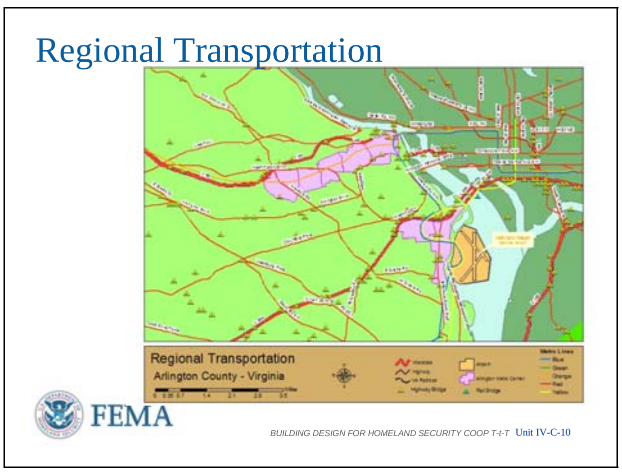
VISUAL IV-C-9



10-Mile Radius

This map displays infrastructure and features within a 10-mile radius that could have an impact on the site. Features mapped include utilities, major transportation networks, first responders, and government facilities.

VISUAL IV-C-10

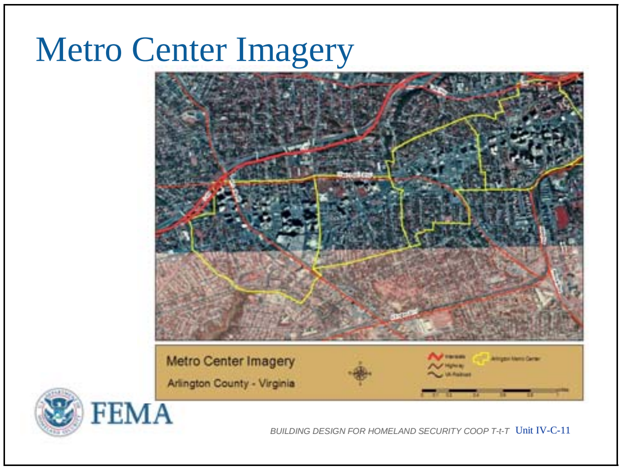


Regional Transportation

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-11



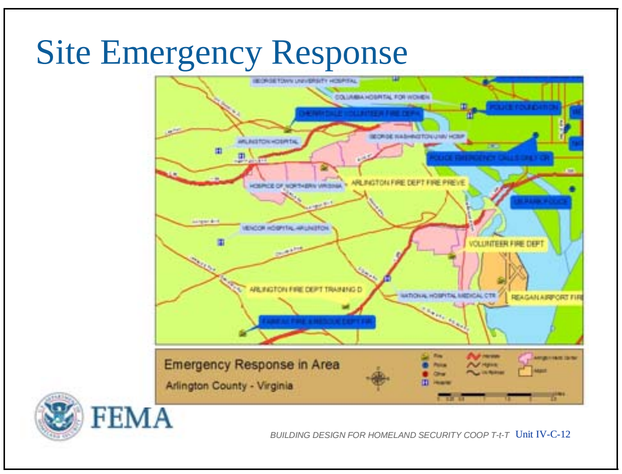
Metro Center Imagery

Satellite imagery of the region surrounding a site provides users an additional perspective to go with the data sets information.

Commercial, industrial, and residential areas can easily be differentiated, as well as rural and urban areas.

This map can be used for an overview of the surrounding area and for determining if collateral damage is a significant risk.

VISUAL IV-C-12

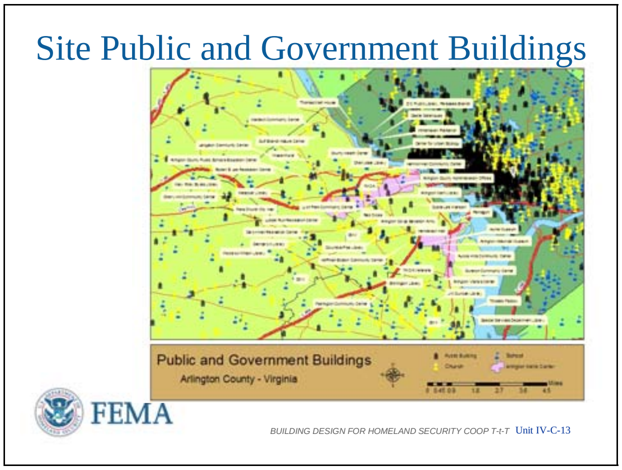


Site Emergency Response

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

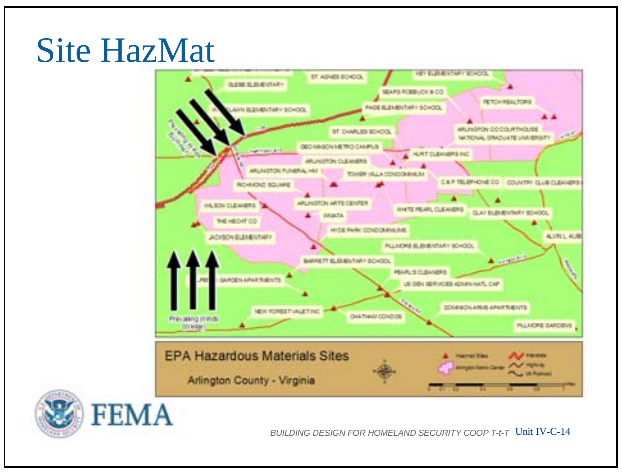
VISUAL IV-C-13



Site Public/Government Buildings

This map shows the location of government and public buildings in the region, including government facilities, schools, and churches. Government buildings potentially could be the target of terrorist operations. Therefore, the possibility of collateral damage should be considered for sites in close proximity. Additionally, some churches and schools may be designated community shelters and resources during emergencies.

VISUAL IV-C-14



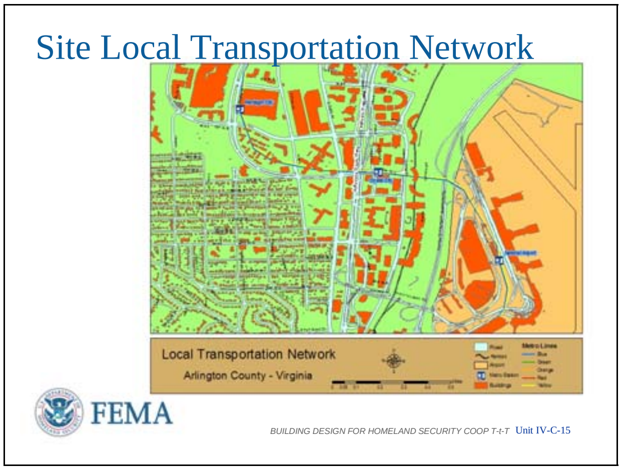
Site HazMat

This map displays hazardous materials (HazMat) sites tracked by various EPA databases. They include large HazMat sites such as refineries and chemical plants, but also include smaller sites with small quantities of chemicals such as schools and dry cleaners. Some sites that contain very small amounts of HazMat are filtered out.

Prevailing wind direction from the National Oceanic and Atmospheric Administration (NOAA) Climatic Data Center is shown to help evaluate the vulnerabilities from surrounding hazards that can be used by a terrorist as a supplemental weapon.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-15



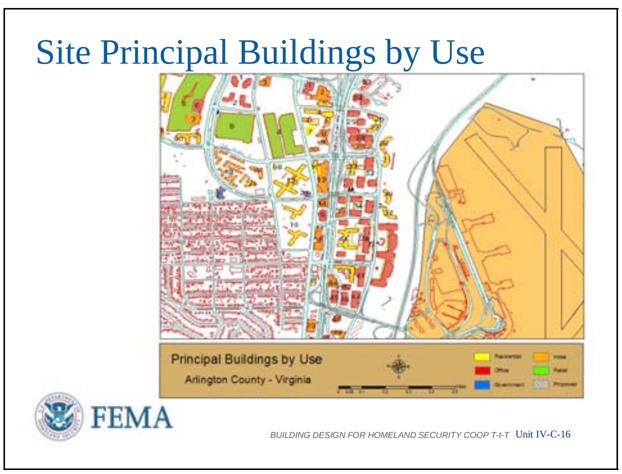
Site Local Transportation Network

The local transportation map provides greater resolution of transportation routes in the local area surrounding a site.

It can be used for planning evacuation routes and alternate routes during an emergency.

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

VISUAL IV-C-16

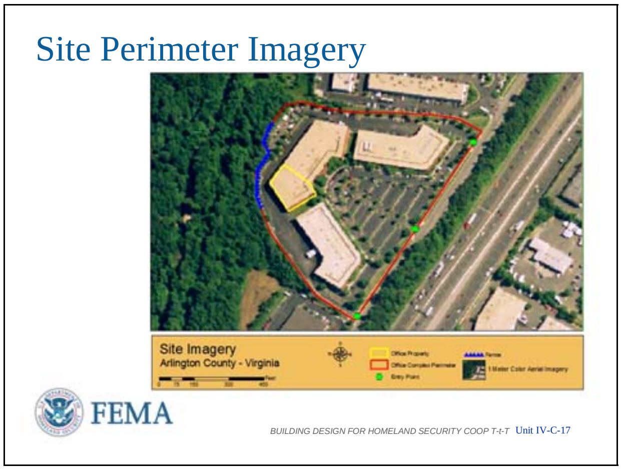


Site Principal Buildings by Use

This map provides a quick overview of the primary use of principal buildings surrounding a site.

It is useful when conducting threat assessments to help identify potential surrounding terrorist targets and the likelihood of collateral damage.

VISUAL IV-C-17

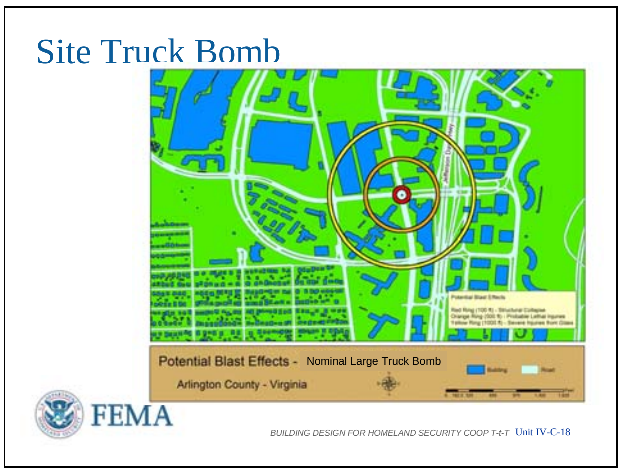


Site Perimeter Imagery

Site imagery gives a view of the site and allows assessors to analyze the layout of the site, including site entry points and building separation.

The imagery can also be integrated with building plans to provide important information for implementing mitigation measures and making other security decisions.

VISUAL IV-C-18



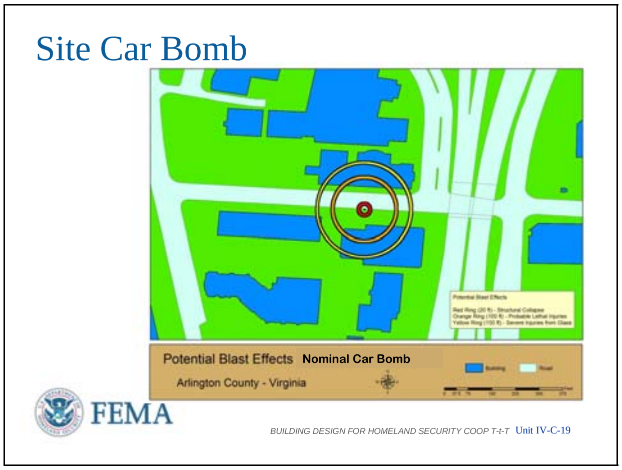
Site Truck Bomb

Displays the potential effects of a nominal truck bomb assuming a nominal building structure.

It is an estimation based on range-to-effects charts and is useful for analyzing vehicular flow and stand-off issues. The results of more accurate site-specific blast analysis can be used to replace the nominal estimations, especially for more accurate cost estimating of mitigation measures.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-19

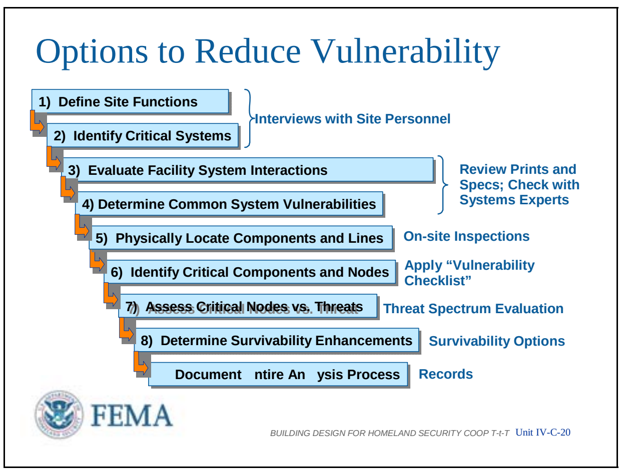


Site Car Bomb

This is an example of the potential blast effects associated with a nominal car bomb against a building with nominal construction.

Obviously, the effects of the car bomb are much less than those from a truck bomb.

VISUAL IV-C-20



Options to Reduce Vulnerability

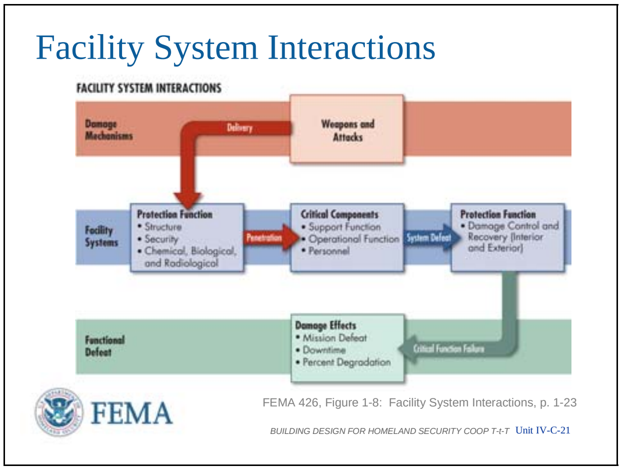
After identifying and collecting information on the site, the multidisciplinary team follows the nine steps listed here:

1. Define Site Functions
2. Identify Critical Systems
3. Evaluate Facility System Interactions
4. Determine Common System Vulnerabilities
5. Physically Locate Components and Lines
6. Identify Critical Components and Nodes
7. Assess Critical Nodes Versus Threats
8. Determine Survivability Enhancements (and Options) [Mitigation measures]
9. Document Entire Analysis Process [To avoid having to recreate it, but moreso to allow adjustments as threats change and as mitigation measures are implemented so as to track the current state if an attack should occur.]

This process is explained in more detail in FEMA 452. For this course, this is an overview of what a more detailed on-site assessment should accomplish.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-21



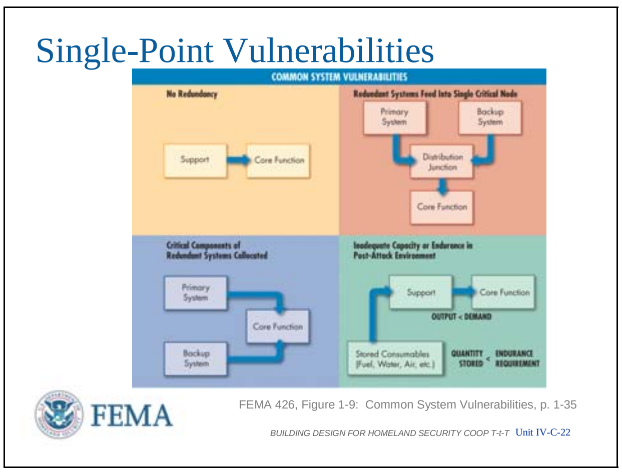
Facility System Interactions

Every building or facility can be attacked and damaged or destroyed as illustrated in the flow chart.

A terrorist selects the weapon and tactic that will destroy the building or infrastructure target.

At a site with multiple buildings, **Tables 1-5 through 1-17 in FEMA 426** can be used to <u>rank order</u> these buildings and thus to determine which buildings require more in-depth analysis.

VISUAL IV-C-22



Single-Point Vulnerabilities are critical functions or systems that lack redundancy and, if damaged by an attack, would result in immediate organization disruption or loss of capability.

<u>COOP</u>: SPVs are equally important to the continued functioning of alternate facilities.

Single-Point Vulnerabilities (SPVs)

The function and infrastructure analysis will identify the <u>geographic distribution</u> within the building and <u>interdependencies between critical assets</u>. Ideally, the functions should have geographic dispersion as well as a recovery site or alternate work location. However, some critical building functions and infrastructure do not have a backup, or will be found collocated. This design creates what is called a Single-Point Vulnerability.

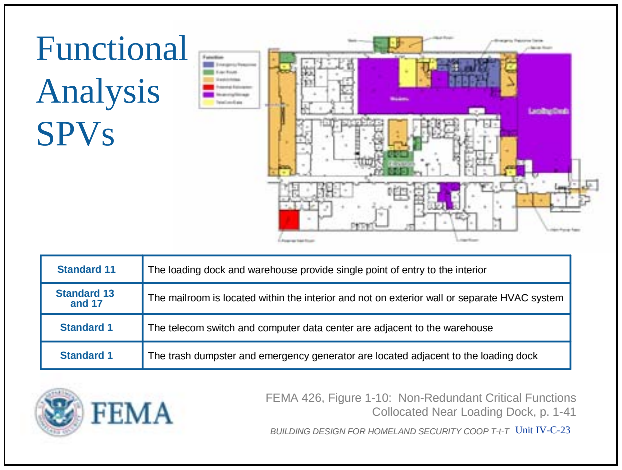
<u>Identification and protection of these Single-Point Vulnerabilities is a key aspect of the assessment process.</u>

This chart provides examples of this concept:

1. No Redundancy
2. Redundant Systems Feed Into Single Critical Node
3. Critical Components of Redundant Systems Collocated
4. <u>Inadequate Capacity or Endurance in Post-Attack Environment</u>

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-23



Functional Analysis SPVs

There are both Functional Analysis SPVs and Infrastructure SPVs.

Functional Analysis SPVs are depicted in this chart. This figure shows an example of a building that has numerous critical functions and infrastructure collocated, which creates a single-point vulnerability.

VISUAL IV-C-24

Infrastructure Analysis SPVs

Typical infrastructure SPVs are depicted here:

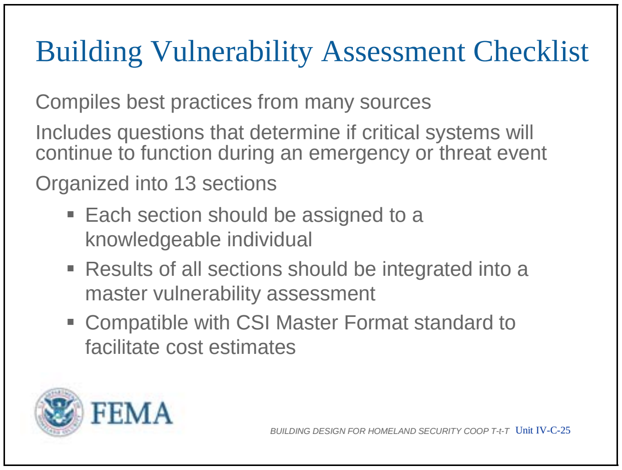
- Air intakes at ground level
- Ground level drive through drop-off atrium with no anti-vehicle barrier
- Single primary electrical service
- Single telecom switch room in parking garage

Many commercial buildings have collocated electrical, mechanical, and telecom rooms that share a common central distribution core or chase.

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-25



The **Building Vulnerability Assessment Checklist** is based on a checklist developed by the Department of Veterans Affairs (VA). The checklist can be used as a screening tool for preliminary design vulnerability assessment. In addition to examining design issues that affect vulnerability, the checklist includes questions that determine if critical systems continue to function in order to enhance deterrence, detection, denial, and damage limitation, and to ensure that emergency systems function during and after a threat or hazard situation.

Building Vulnerability Assessment Checklist

FEMA 426 provides the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93)**, which compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building.

This helps guide the multidisciplinary team through the vulnerability analysis. It allows a consistent security evaluation of designs at various levels, whether accomplished as owner/user or in-depth with technical experts.

The assessment checklist has been used by experienced engineers who were not experienced vulnerability assessors. These engineers commented that although the checklist seemed laborious at first, when they finished assessing multiple sites across the country they felt very confident that they had identified the vulnerabilities and had provided solid recommendations for mitigation measures.

The CSI (Construction Specification Institute) format has other advantages that designers and engineers can develop detailed specifications that communicate requirements to building contractors.

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-26

Building Vulnerability Assessment Checklist

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

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-26

Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Each section of the checklist can be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area in order to perform a detailed assessment.

As stated before, an initial assessment can be performed by craftsmen and other knowledgeable people that may provide the decision maker all that is necessary or indicate more expertise is needed in specific areas.

VISUAL IV-C-27

Building Vulnerability Assessment Checklist

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

FEMA

FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92

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

Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. Not all possible questions are in the checklist, but it provides a good basis to guide the assessment.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-28

Building Vulnerability Assessment Checklist

1.15	Is there minimum setback distance between the building and parked cars?
4.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?
4.2	Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)?

FEMA

FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-28

VISUAL IV-C-29

Building Vulnerability Assessment Checklist

2.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?
1.16	Does adjacent surface parking on site maintain a minimum stand-off distance? ***For initial screening consider using 25 meters (82 feet) as a minimum with more distance needed for unreinforced masonry or wooden walls. Reference: GSA PBS-P100***

FEMA

FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-29

Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Notice that the checklist leads assessment team members to see the same critical functions or infrastructure from different perspectives.

For example, here a parking lot is analyzed by questions from both the site and building envelope sections. (Sections 1 and 4)

This cross analysis is one of the strengths of the methodology.

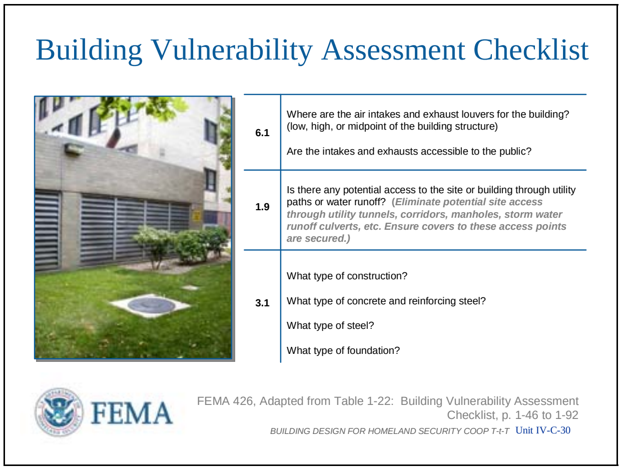
Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

In this example, the same function, a loading dock, is addressed by different sections (Sections 1 and 2 – Site and Architectural).

The location of the trash dumpster, building overhang, and exposed loading dock columns make this area susceptible to significant blast damage.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-30

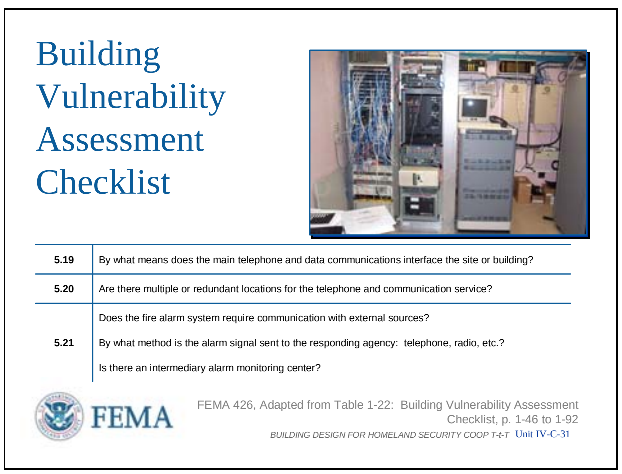


Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

In this example, the same feature, an air intake, is addressed by questions from three sections:

- #1 – Site
- #3 – Structural Systems
- #6 – Mechanical Systems

VISUAL IV-C-31



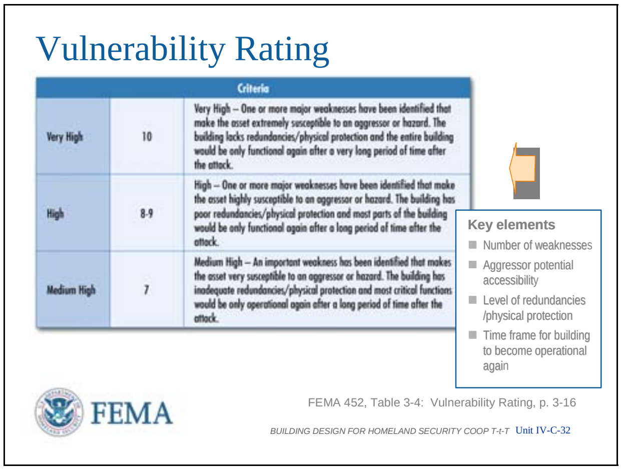
Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Section 5 of the **Building Vulnerability Assessment Checklist** addresses Utility Systems.

Utility systems are normally that portion of utilities that is outside the building. However, the demark (demarcation line) can be just inside the building. Up to this point is the responsibility of the utility company. After the demark is part of the building and is handled by other sections in the Building Vulnerability Assessment Checklist.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-32



Vulnerability Rating (1/2)

The results of the 13 assessment sections should be integrated into a master vulnerability assessment in order to provide the basis for determining vulnerability rating numeric values.

In the rating scale of 1 to 10, a rating of 10 means one or more major weaknesses exist to make an asset extremely susceptible to an aggressor's tactics.

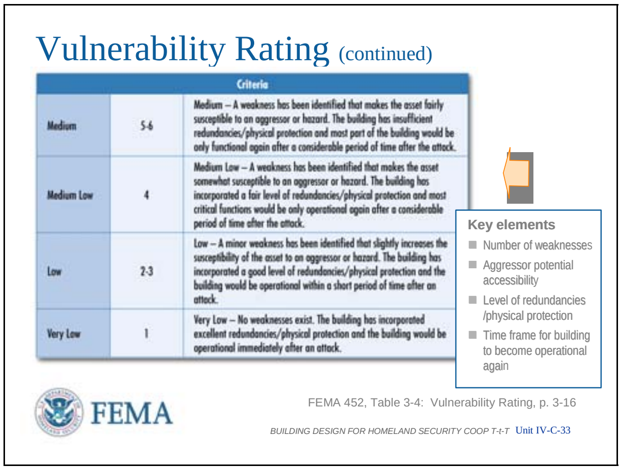
- **Very High –** One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The building lacks redundancies/physical protection and will not be functional again after an attack.

- **High –** One or more significant weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The building has poor redundancies/physical protection and most parts of the building will not be operational until 1 year after an attack.

- **Medium High –** An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The building has inadequate redundancies/physical protection and some critical functions will not be operational until 9 months after an attack.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-33



Vulnerability Rating (2/2)

On the other end of the vulnerability rating scale is the rating of 1 which means very low and no weaknesses exist.

- **Medium –** A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The building has insufficient redundancies/physical protection and some critical functions will not be operational until 6 months after an attack.

- **Medium Low –** A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard. The building has incorporated a fair level of redundancies/physical protection and the building will be operational 3 months after an attack.

- **Low –** A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated good redundancies/physical protection and will be operational a few weeks after an attack.

- **Very Low –** No weaknesses exist. The building has incorporated excellent redundancies/physical protection and will be operational immediately after an attack.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-34

Critical Functions

Function	Cyber attack	Armed attack (single gunman)	Vehicle bomb	CBR attack
Administration				
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	**7**	**7**	**9**	**9**
Engineering				
Asset Value	8	8	8	8
Threat Rating	8	5	6	2
Vulnerability Rating	**2**	**4**	**8**	**9**

FEMA

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

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-34

The Vulnerability Rating is subjective and the assessor has to take into account how well the asset is protected against that threat, if redundancy is in place, and the effect of the tactics and weapons against the asset as it currently exists.

Critical Functions Matrix

The Vulnerability Rating is entered into the same Critical Functions that we saw in Units II and III.

The Vulnerability Ratings under the Administration Function and under the Engineering Function are highlighted.

Since vulnerability is a measure of the success and effects of employing a threat against asset, the vulnerability varies based upon location, hardening, ability to use the tactic, redundancy, etc.

A medium-high (7) and high (9) Vulnerability Rating was assigned to the Administration Function threat pairs to illustrate an exposed function near exterior walls and entrances.

A range of ratings was assigned for the Engineering Function threat pairs to illustrate a function that is typically in the interior core, but shares common HVAC systems and is likely within a blast damage zone based upon the potential weapon size.

VISUAL IV-C-35

Critical Infrastructure

Infrastructure	Cyber attack	Armed attack (single gunman)	Vehicle bomb	CBR attack
Site				
Asset Value	4	4	4	4
Threat Rating	4	4	3	2
Vulnerability Rating	**1**	**7**	**9**	**9**
Structural Systems				
Asset Value	8	8	8	8
Threat Rating	3	4	3	2
Vulnerability Rating	**1**	**1**	**8**	**1**

FEMA

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

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-35

Critical Infrastructure Matrix

The Vulnerability Rating is entered into the same Critical Infrastructure Matrix that we saw in Units II and III.

The Vulnerability Ratings under the Site and Structural Systems are highlighted.

NOTE: It is easier to keep the threat in mind and move between assets to assess vulnerability than it is to keep the asset in mind and move between threats.

Cyber Attack: Rating of 1 for both.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

- Site: Rating of 1 as no internet connected system in place, like a perimeter access control system, or connection to other accessible media (phone lines).
- Structural: Rating of 1 as no electronic systems at all, but could have an active damping system for earthquake or high winds that is accessible over the internet which would give it a rating higher than 1

Armed Attack:

- Site: Rating of 7 as it is fairly open, but with some obscuration, many manned windows overlooking the parking lots, CCTV coverage, and roving patrols at variable times
- Structural: Rating of 1 as this tactic would have no impact upon the structural members

Vehicle Bomb

- Site: Rating of 9 as a vehicle bomb would cause extensive destruction to site and hinder operations for extended time due to limited access and blowing debris damage to buildings
- Structural: Rating of 8 as building is a high-rise and not designed for progressive collapse, but stand-off provides some level of protection.

CBR Attack

- Site: Rating of 8, because depending upon agent used the access to site could be restricted from hours to years or until decontamination is complete, which would not be a speedy process
- Structural: Rating of 1 as agent would not restrict structural system in any fashion in performance of its engineered design

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-C-36

Summary

Step-by-Step Analysis Process:

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

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-36

Summary

- Expertise and experience as required for the level of assessment and the criticality of the building
- Dig deeper in identifying Critical Functions and Critical Infrastructure as the systems interfaces are better understood
- Apply understanding of threats as they interact with assets to identify vulnerabilities and understand benefit of selected mitigation measures
- Apply vulnerability ratings to the Critical Functions and the Critical Infrastructure Matrices based upon how that threat can interact and impact that asset.

VISUAL IV-C-37

Vulnerability Rating Considerations

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

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

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

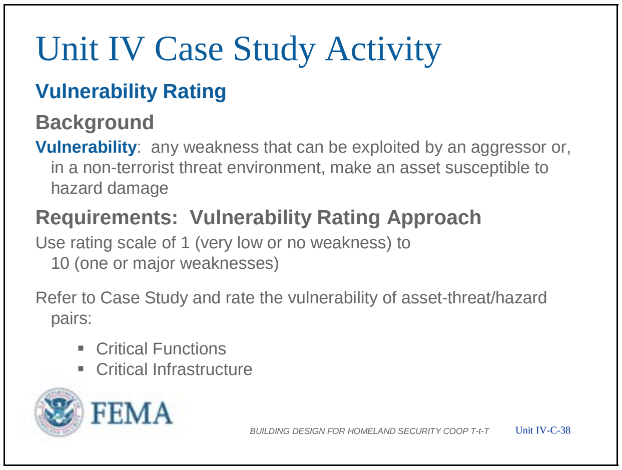
Vulnerability Rating Considerations

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

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

INSTRUCTOR NOTES

VISUAL IV-C-38



Refer students to the Unit IV Case Study activity in the Student Manual.

At the end of the working session (35 minutes), reconvene the class and facilitate group reporting (plenary group 10 minutes).

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

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

CONTENT/ACTIVITY

Student Activity

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

Discussion Question

What indicators do you look for to determine if any vulnerability exists in the building design?

Suggested Responses:

- *Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability").*
- *Redundant systems feeding into a single critical node.*
- *Critical components of redundant systems collocated.*
- *Inadequate capacity or endurance in post-attack environment.*

Activity Requirements:

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

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

Take 35 minutes to complete this part of the

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	activity.

Transition

Unit V will cover Risk Assessment/Risk Management and complete instruction on the risk assessment process. Unit VI will present the FEMA 452 Risk Assessment database as an improvement over the manual process.

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

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

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

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

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

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

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

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

- Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability")
- Redundant systems feeding into a single critical node
- Critical components of redundant systems collocated
- Inadequate capacity or endurance in post-attack environment

Vulnerability rating requires identifying and rating the vulnerability of each asset-threat/hazard pair of interest. In-depth vulnerability assessment of a building evaluates specific design and architectural features and identifies all vulnerabilities of the building functions and building systems.

Vulnerability Rating Activities

1. Complete the tables for Critical Functions and Critical Infrastructure Vulnerability Ratings.
    - Some ratings and rationale are provided as **examples**.
    - Adjust ratings as desired by team consensus and provide rationale for the provided or adjusted ratings as appropriate.
    - Refer to the Appendix C Case Study as needed.

2. Transfer the vulnerability ratings to the Risk Matrix poster after reaching team consensus on the answers.

CI/BC Critical Functions Vulnerability Ratings

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

RATIONALE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Middle:

Low End:

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

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

Middle:

Low End:

CI/BC Critical Infrastructure Vulnerability Ratings

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

RATIONALE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Low End:

CBR Attack is also global, but takes into account the effect of the CBR agents on the equipment, its operation, and the accessibility of operations and maintenance personnel to ensure system operations.

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

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

Middle:

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

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

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

Unit V (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 45 minutes
UNIT TITLE	Risk Assessment / Risk Management
OBJECTIVES	1. Explain what constitutes risk. 2. Provide a numerical rating for risk and justify the basis for the rating. 3. Evaluate risk using the Risk (Threat-Vulnerability) Matrix to capture assessment information. 4. Identify top risks for asset-threat/hazard pairs of interest that should receive measures to mitigate vulnerabilities and reduce risk.
SCOPE	The following topics will be covered in this unit: 1. Definition of risk and the various components to determine a risk rating. 2. The FEMA 426 approach to determining risk. 3. A rating scale and how to use it to determine a risk rating. One or more specific examples will be used to focus students on the following activity. 4. The relationships between high risk, the need for mitigation measures, and the need to identify a Design Basis Threat and Level of Protection. 5. Activity: Determine the risk rating for the asset-threat/hazard pairs of interest. Identify the high risk ratings for the Case Study.
REFERENCES	1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-35 to 1-44 2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 4-1 to 4-9 3. Case Study – Appendix C: COOP, Cooperville Information / Business Center 4. Student Manual, Unit V(C) (info only – not listed in SM) 5. Unit V (C) visuals (info only – not listed 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 V (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit V (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

UNIT V (C) OUTLINE

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.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The student activity is primarily a math exercise in multiplying the asset value, threat, 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 assessment to focus attention on specific vulnerabilities as an input to select mitigation measures.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page (Unit #) in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- Explain that the 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, <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.

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

(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

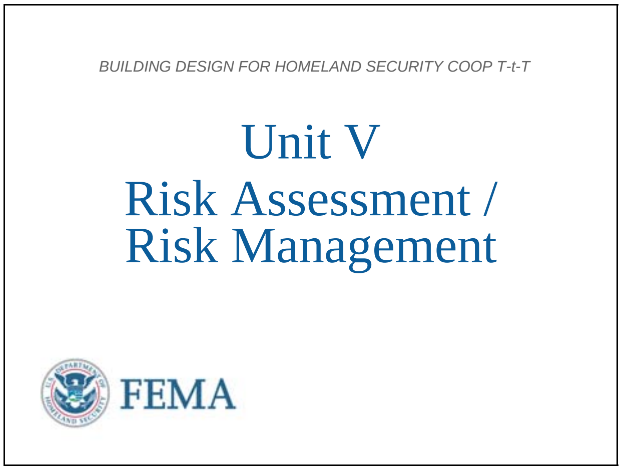
(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-C-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-C-2

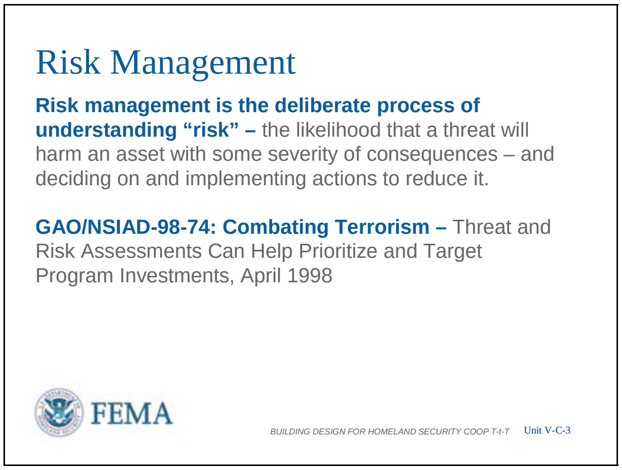
Unit Objectives

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

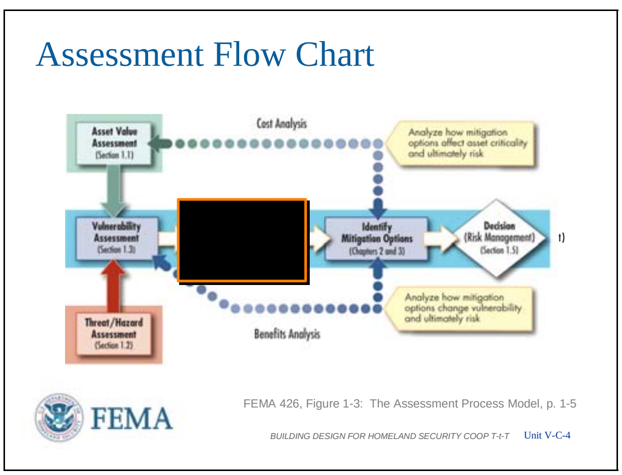
1. Explain what constitutes risk.
2. Provide a numerical rating for risk and justify the basis for the rating.
3. Evaluate risk using the Risk Matrix poster (Threat-Vulnerability Matrix) to capture assessment information.
4. Identify top risks for asset-threat/hazard pairs of interest that should receive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

INSTRUCTOR NOTES

VISUAL V-C-3



VISUAL V-C-4



CONTENT/ACTIVITY

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, <u>realize that risk reduction has two other components, albeit not applicable to building design</u>:

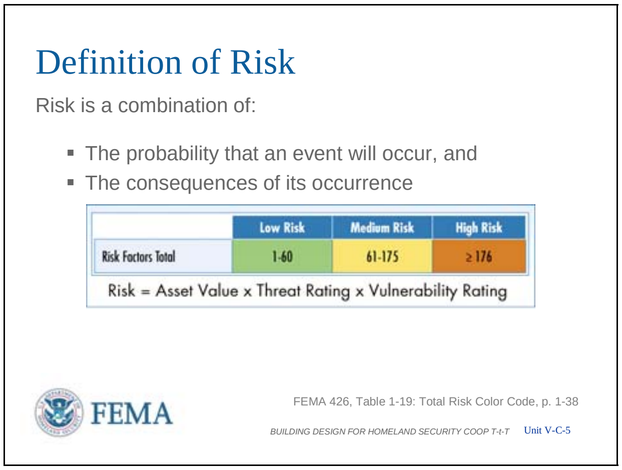
- Reduce asset value (<u>Devalue</u> the asset)
- Reduce threat (intelligence and law enforcement team to arrest terrorists before an attack can be carried out)

Assessment Flow Chart

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-C-5

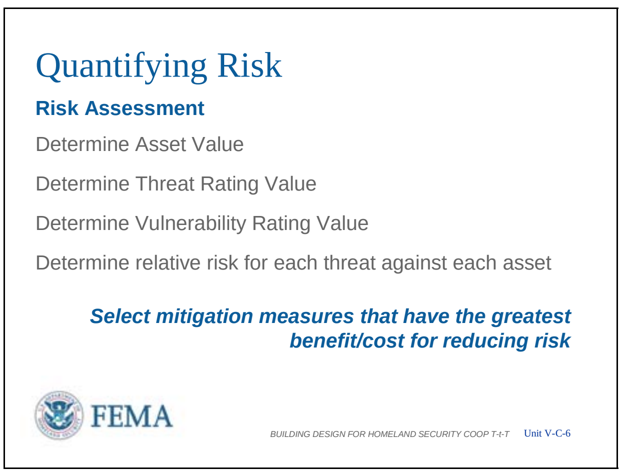


Risk

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-C-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.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL V-C-7

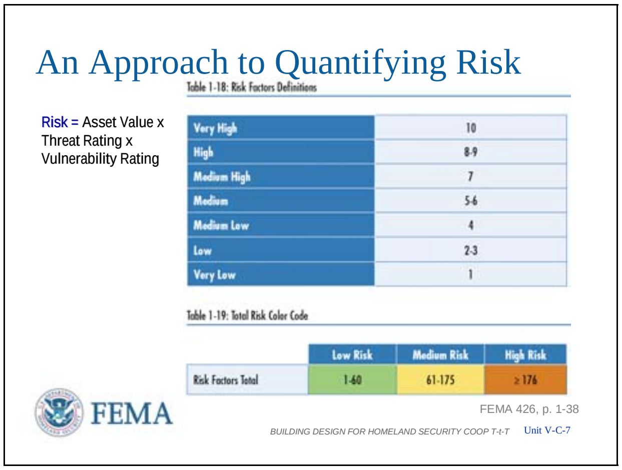


Table 1-18: Risk Factors Definitions

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

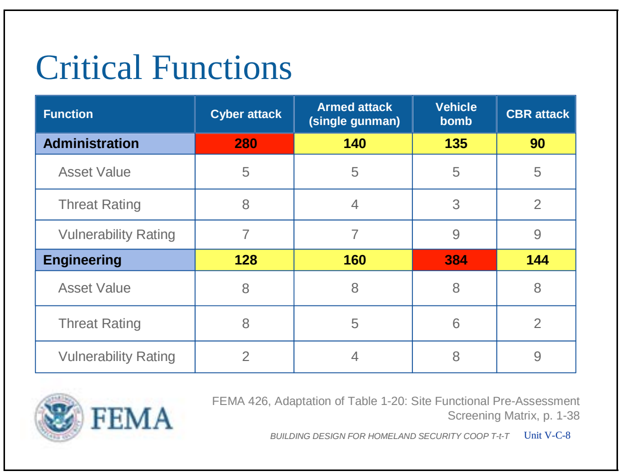
An Approach to Quantifying Risk

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.)**

VISUAL V-C-8



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

Critical Functions Matrix

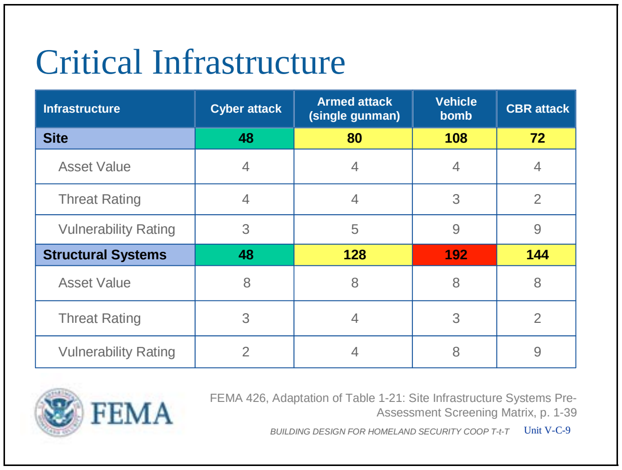
This analysis completes the Critical Functions and the Critical Infrastructure Matrices that we saw in Units II, III, and IV.

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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-C-9



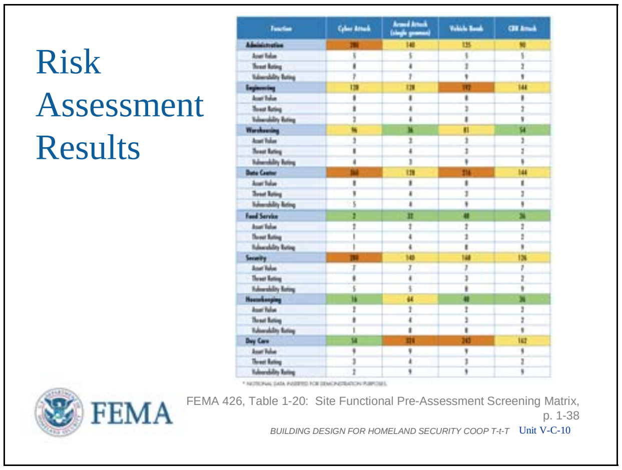
Critical Infrastructure

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

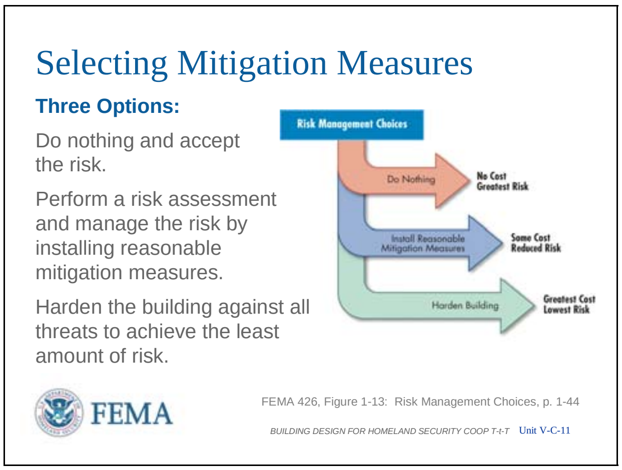
INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

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.

VISUAL V-C-11



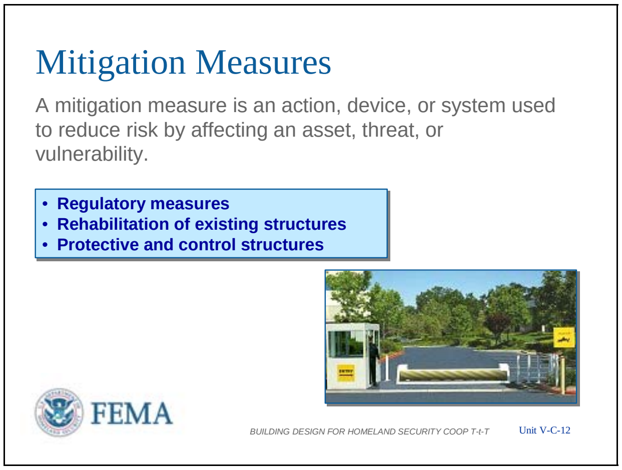
Selecting Mitigation Measures

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

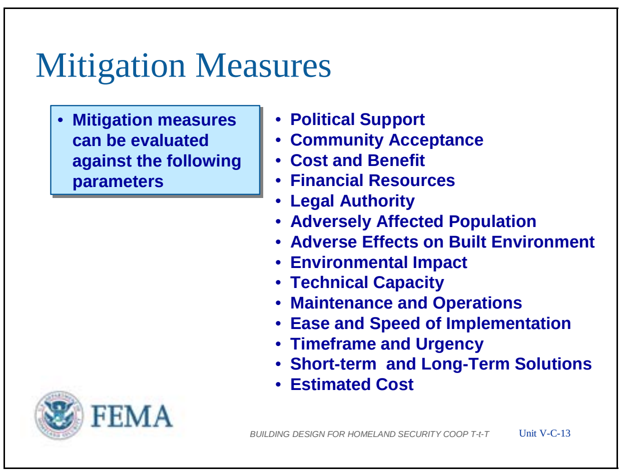
1. Do nothing and accept the risk (no cost).
2. Perform a risk assessment and manage the risk by installing reasonable mitigation measures (some cost).
3. <u>Harden the building against all threats to achieve the least amount of risk (but at greatest cost).</u>

INSTRUCTOR NOTES

VISUAL V-C-12



VISUAL V-C-13



CONTENT/ACTIVITY

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.

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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-C-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-C-15

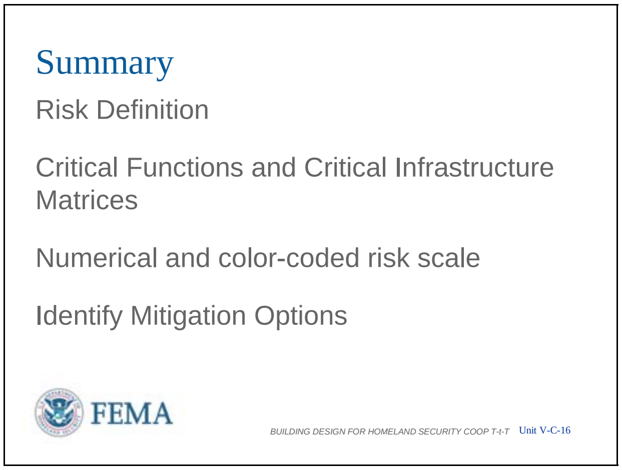
Process Review

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

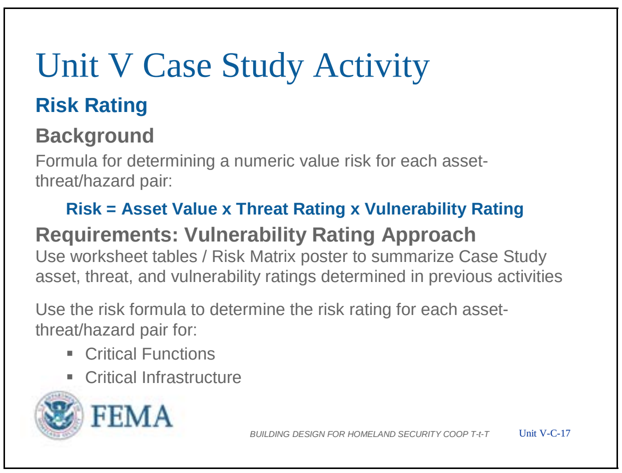
To get the maximum benefit from limited resources, realize that certain mitigation measures can reduce risk for multiple, high-risk asset – threat / hazard pairs.

INSTRUCTOR NOTES

VISUAL V-C-16



VISUAL V-C-17



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).

CONTENT/ACTIVITY

Summary

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

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:

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

Activity Requirements

Working with your team, use the worksheet tables or Risk Matrix poster to summarize the asset, threat, and vulnerability assessment ratings determined in the previous three unit student activities for the selected Case Study.

Ensure the answers are a team consensus.

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

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	Circle all High risk ratings using a RED whiteboard marker. Take 15 minutes to complete this 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 (C) CASE STUDY ACTIVITY: RISK RATINGS (COOP 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:

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

Requirements

1. Use the following worksheet tables or the Risk Matrix poster to summarize the CI/BC asset value, threat/hazard, and vulnerability assessment ratings conducted in the previous three unit activities. Reach team consensus on answers.

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

3. Transfer the ratings to the Risk Matrix poster and circle all high risk ratings in RED using a whiteboard marker.

CI/BC Critical Functions Risk Ratings

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. **Administration Risk Rating**	*128*	*96*	*192*	*128*
Asset Value Rating	*4*	*4*	*4*	*4*
Threat Rating	*8*	*3*	*6*	*4*
Vulnerability Rating	*4*	*8*	*8*	*8*
2. **Engineering/IT Technicians Risk Rating**	*256*	*144*	*384*	*256*
Asset Value Rating	*8*	*8*	*8*	*8*
Threat Rating	*8*	*3*	*6*	*4*
Vulnerability Rating	*4*	*6*	*8*	*8*
3. **Loading Dock/ Warehouse Risk Rating**	*64*	*96*	*192*	*128*
Asset Value Rating	*4*	*4*	*4*	*4*
Threat Rating	*8*	*3*	*6*	*4*
Vulnerability Rating	*2*	*8*	*8*	*8*

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
4. **Data Center** **Risk Rating**	***240***	***90***	***480***	***320***
Asset Value Rating	***10***	***10***	***10***	***10***
Threat Rating	***8***	***3***	***6***	***4***
Vulnerability Rating	***3***	***3***	***8***	***8***
5. **Communications** **Risk Rating**	***576***	***81***	***432***	***288***
Asset Value Rating	***9***	***9***	***9***	***9***
Threat Rating	***8***	***3***	***6***	***4***
Vulnerability Rating	***8***	***3***	***8***	***8***
6. **Security** **Risk Rating**	***224***	***126***	***336***	***224***
Asset Value Rating	***7***	***7***	***7***	***7***
Threat Rating	***8***	***3***	***6***	***4***
Vulnerability Rating	***4***	***6***	***8***	***8***
7. **Housekeeping** **Risk Rating**	***8***	***6***	***48***	***24***
Asset Value Rating	***1***	***1***	***1***	***1***
Threat Rating	***8***	***3***	***6***	***4***
Vulnerability Rating	***1***	***2***	***8***	***8***

CI/BC Critical Infrastructure Risk Ratings

Infrastructure	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. **Site** **Risk Rating**	***4***	***96***	***192***	***128***
Asset Value Rating	***4***	***4***	***4***	***4***
Threat Rating	***1***	***3***	***6***	***4***
Vulnerability Rating	***1***	***8***	***8***	***8***
2. **Architectural** **Risk Rating**	***5***	***120***	***240***	***20***
Asset Value Rating	***5***	***5***	***5***	***5***
Threat Rating	***1***	***3***	***6***	***4***
Vulnerability Rating	***1***	***8***	***8***	***1***
3. **Structural Systems** **Risk Rating**	***4***	***96***	***384***	***16***
Asset Value Rating	***4***	***4***	***8***	***4***
Threat Rating	***1***	***3***	***6***	***4***
Vulnerability Rating	***1***	***8***	***8***	***1***

Infrastructure	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
4. **Envelope Systems** **Risk Rating**	*5*	*120*	*240*	*20*
Asset Value Rating	*5*	*5*	*5*	*5*
Threat Rating	*1*	*3*	*6*	*4*
Vulnerability Rating	*1*	*8*	*8*	*1*
5. **Utility Systems** **Risk Rating**	*125*	*175*	*180*	*40*
Asset Value Rating	*5*	*5*	*5*	*5*
Threat Rating	*5*	*5*	*6*	*4*
Vulnerability Rating	*5*	*7*	*6*	*2*
6. **Mechanical Systems** **Risk Rating**	*200*	*200*	*384*	*256*
Asset Value Rating	*8*	*8*	*8*	*8*
Threat Rating	*5*	*5*	*6*	*4*
Vulnerability Rating	*5*	*5*	*8*	*8*
7. **Plumbing and Gas Systems** **Risk Rating**	*6*	*36*	*288*	*24*
Asset Value Rating	*6*	*6*	*6*	*6*
Threat Rating	*1*	*3*	*6*	*4*
Vulnerability Rating	*1*	*2*	*8*	*1*
8. **Electrical Systems** **Risk Rating**	*200*	*48*	*384*	*24*
Asset Value Rating	*8*	*8*	*8*	*8*
Threat Rating	*5*	*3*	*6*	*4*
Vulnerability Rating	*5*	*2*	*8*	*1*
9. **Fire Alarm Systems** **Risk Rating**	*20*	*30*	*240*	*20*
Asset Value Rating	*5*	*5*	*5*	*5*
Threat Rating	*2*	*3*	*6*	*4*
Vulnerability Rating	*2*	*2*	*8*	*1*
10. **IT/Communications Systems** **Risk Rating**	*630*	*54*	*432*	*288*
Asset Value Rating	*9*	*9*	*9*	*9*
Threat Rating	*10*	*3*	*6*	*4*
Vulnerability Rating	*7*	*2*	*8*	*8*

During plenary session ask the assessment teams what they have identified as their highest risks. Using the school solutions presented in previous student activities, the top three risks are as follows:

Risk #1: Cyber Attack upon IT/Communications (630 / 576)

Risk #2: Vehicle Bomb upon Data Center and Communications (480 / 432), but all Functions and Infrastructure is High Risk

Risk #3: CBR Attack upon Data Center, Communications, Engineering/IT Technicians, and Mechanical Systems (320 / 288 / 256)

Unit VI (C)

COURSE TITLE

Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer

TIME **75** minutes

UNIT TITLE

FEMA 452 Risk Assessment Database

OBJECTIVES

1. Explain the database install process as appropriate.
2. Identify where to save photos, maps, drawings, plans, etc. to interface with the database.
3. Explain the information required for the database to function within each screen, how to move between screens, and switch between the assessment tool operating mode and the master database operating mode.
4. Explain the benefit and approaches to setting priorities on identified vulnerabilities.
5. Explain how to use the database to produce standard reports and search the database for specific information.

SCOPE

The following topics will be covered in this unit:

1. The installation of the FEMA 452 Risk Assessment Database if not previously loaded before arrival for class.
2. Inputting data into the database and linking associated information, such as GIS images, Miscellaneous files, and Photos.
3. Navigation in the database to operate all functions.
4. Risk management capability using the database.
5. Activity: Students will follow the instruction unit.
   Option 1: In a demonstration / performance mode, follow the instruction unit, installing the databases, and navigating the databases following the instructor's presentation.
   Option 2: Install the databases and navigate them outside the instruction unit at some time on Day 2.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 1
2. FEMA 452, *Risk Assessment - A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 4-1 to 4-10
3. FEMA 452 Risk Assessment Database CD with Install Wizard (latest version)

4. Student Manual, Unit VI (C) (info only – not in SM)
5. Unit VI (C) 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 VI (C)
4. FEMA 452 Risk Assessment Database CD with Install Wizard (latest version)
5. Overhead projection or computer display unit
6. Unit VI (C) visuals

UNIT VI (C) OUTLINE

15. Close Assessment Tool	0.5 minute	IG VI-C-55
16. Empty Assessment Database	1 minute	IG VI-C-56
17. Switch to Master Database Mode	2 minutes	IG VI-C-57
18. Master Database Mode	0.5 minute	IG VI-C-58
19. Master Database -- Checklists	1 minute	IG VI-C-58
20. Master Database -- Reports	3 minutes	IG VI-C-60
21. Master Database – Threat Matrix	2 minutes	IG VI-C-62
22. Master Database – Other Reports / Search	3 minutes	IG VI-C-64
23. Master Database – Vulnerability Assessment Checklist	3 minutes	IG VI-C-67
24. Master Database – Changing Passwords	1 minute	IG VI-C-70
25. Master Database – Administrative Functions	2 minutes	IG VI-C-72
26. Master Database – Import Database	6 minutes	IG VI-C-73
27. Master Database – Managing User Accounts	3 minutes	IG VI-C-79
28. Summary, Student Activity, and Transition	1 minute	IG VI-C-82

Preparing To Teach This Unit

- **Tailoring Content to the Local Area:** This instruction unit has no requirement to include any tailoring of content to the Local Area.

- **Software Familiarity**: The instructor for this unit should first read the User Guide for the Version 3.0 database. Then the instructor should understand how to work with the FEMA 452 Risk Assessment Database Version 3.0 by following along with the slides and actually working with the software.

- **Optional Activity:** There are two optional approaches to this unit.

  - **Activity 1:** During this presentation the students with laptops will benefit from a demonstration / performance instruction methodology by actually following along with the instructor and performing the actions installing and navigating the software using the Database CD provided to each student at this class.

- **Activity 2:** Due to problems with laptop administrator rights for loading software in the past, particularly on Federal and State level government computers, do not use demonstration / performance. Walk through the slides to provide the concepts and schedule a time (lunch and/or end of day on Day 2) to assist all those interested in loading the software.

- Refer students to their Student Manual, Unit VI (C), for an explanation of this activity.

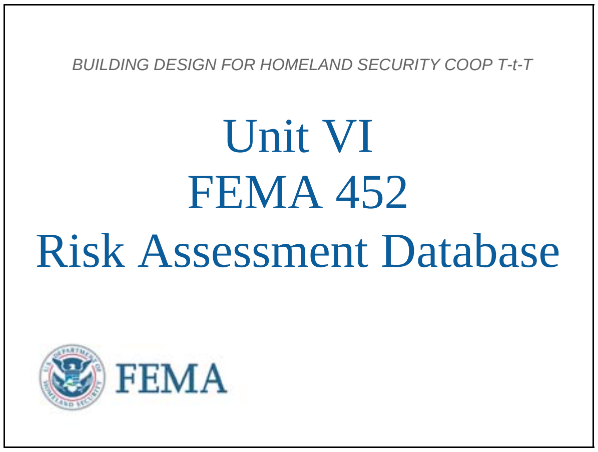
- Ask for and answer questions at the end of this presentation.

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

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

INSTRUCTOR NOTES

VISUAL VI-C-1



NOTE: This Instruction Unit is designed to use FEMA 452 Database Version 3.0 Install Wizard: January 16, 2007.

NOTE to instructor: Minimum System Requirements and how to determine if students have difficulty loading database -- Expect the unexpected

Minimum hardware requirements:

- Pentium® 4 or equivalent
- Windows XP
- 256 MB of RAM recommended for all components

NOTE to instructor: FEMA 452 Database Version 4.0 will be able to work in Windows 2000 and probably Windows Vista in addition to Windows XP.

To Get System Information:

1. Click <Start> in lower left corner of screen
2. Click <Control Panel> near middle of right column
3. Click <System> in icons or detail list
4. Should be on <General> Tab, if not click <General>
5. You should find the hardware information in the right column of

CONTENT/ACTIVITY

Introduction and Unit Overview

Yesterday you performed the risk assessment using manual techniques. This instruction unit shows the database available to collect and analyze the same information, but in a more efficient manner, especially if risk management applies to multiple buildings or sites.

- **NOTE 1**: When the US Army Corps of Engineers used the RAM-D assessment process to assess the 360+ dams the Corps is responsible across the US, the result was three 3-inch binders of information for each dam (over 1,000 binders. For risk management / program management, a database with the results in separate records that allow search and report capability is a better long-term solution.

NOTE 2: There are currently three versions of the database. Version 1.0, which currently comes with the hardcopy FEMA 452 publication (inside back cover), needs an IT Professional and/or a Database Manager (DBM) / Database Administrator (DBA) to configure the database on a server for use by many persons simultaneously and to move data between Assessment Tool and the Master Database. Version 2.0, does not require an IT Professional / Database Administrator / or Database Manager to perform most functions. It can handle a limited number of users accessing the master database at one time. It is designed for the Assessor or Program Manager who does not have the IT or Database expertise on staff that is needed by Version 1.0. Version 3.0, the one being presented here is an improvement of Version 2. It adds COOP facility assessment guidance, a COOP related checklist, an expanded list of facility information, and the ability to manage user accounts and change passwords.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

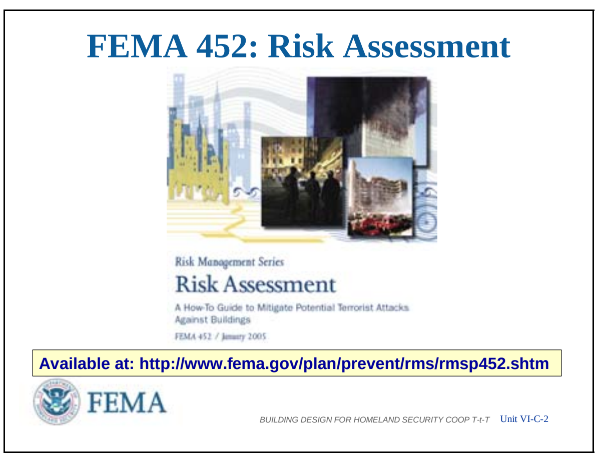
that screen

<u>Minimum software requirements</u>:
MS Access® 2002

NOTE to instructor: FEMA 452 Database Version 4.0 will be able to work in Microsoft Access 2000 and, possibly the Microsoft Vista version of Access in addition to Microsoft Access 2002 and later versions. This is due to removing "References" that are different for each version of Access.

1. Click <Start> in lower left corner of screen
2. Click <All Programs> in the lower left corner
3. Click <MS Access> -- Look for it
4. In Access click <Help> Tab, the last tab on the right at the top of the screen
5. Click <About MS Access> found at the bottom of the pull-down menu
6. Find the version of MS Access at the top of the screen

VISUAL VI-C -2



Introduction and Unit Overview

To support the facility assessment process, an easy to use Risk Assessment Database application is provided in conjunction with FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*.

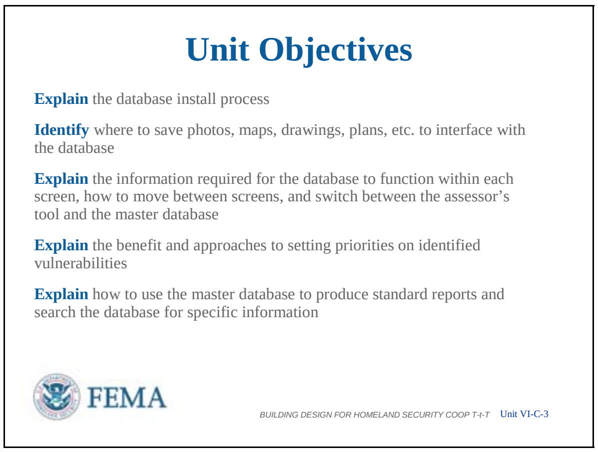
The Risk Assessment Database is a standalone application that is both a data collection tool and a data management tool. Assessors can use the tool to assist in the systematic collection, storage and reporting of assessment data. It has functions, folders and displays to import and display threat matrices, digital photos, cost data, site plans, floor plans, emergency plans, and certain GIS products as part of the record of assessment.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Managers can use the application to store, search and analyze data collected from multiple assessments, and then print a variety of reports.

The FEMA 452 publication is available at the URL shown.

VISUAL VI-C -3



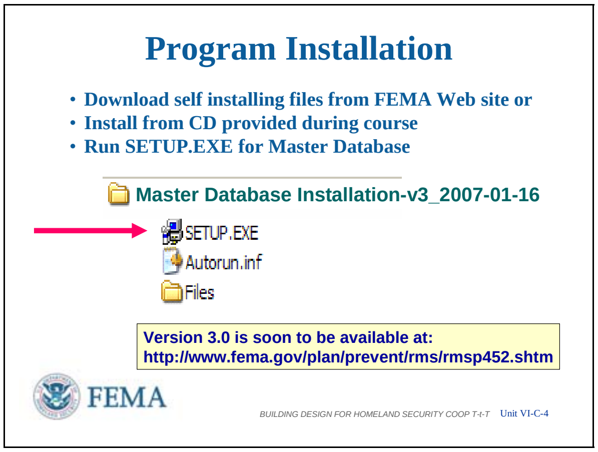
Unit Objectives

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

- **Explain** the database install process
- **Identify** where to save photos, maps, drawings, plans, etc. to interface with the database
- **Explain** the information required for the database to function within each screen, how to move between screens, and switch between the Assessment Tool operating mode and the Master Database operating mode.
- **Explain** the benefit and approaches to setting priorities on identified vulnerabilities
- **Explain** how to use the master database operating mode to produce standard reports and search the database for specific information

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C -4
HIDDEN SLIDE



Program Installation – Assessment Tool

The first task is to download and install the database program from the FEMA website or from the CD provided during this course. Follow the download and self installation instructions. Note that the previous version had two separate databases while Version 3.0 is only one database with two different operating modes.

Install one copy of the program as the Master Database on a computer at your organization's headquarters. This will act as the permanent database that stores assessments, produces reports, and is used to manage the assessment program. This is installed one time and is the permanent program. This database is normally run in the Master Database operating mode.

Install a second copy of the program to use in the Assessment Tool operating mode on the computer(s) that your assessors will use to collect data, such as a laptop. This is intended to be a temporary database that can be used to collect data, pass the collected data on to the Master Database, and then have its records deleted so it can be used for other assessments. This database is normally run in the Assessment Tool operating mode.

We begin the installation process by Left Clicking on SETUP.EXE for the database.

The normal way to install a program is to close all other programs, then:

- Left Click on <Start>
- Left Click on <Run>
- Browse to identify the location where the SETUP.EXE program can be found (CD, C:/Temp, or some other storage location on hard drive or media) and

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Left Click on <OK>

Currently Version 2.0 is available for download from the indicated web site, with Version 3.0 to be added some time in the near future (Spring 2007). Version 4.0 adding Natural Hazards will be available later in 2007.

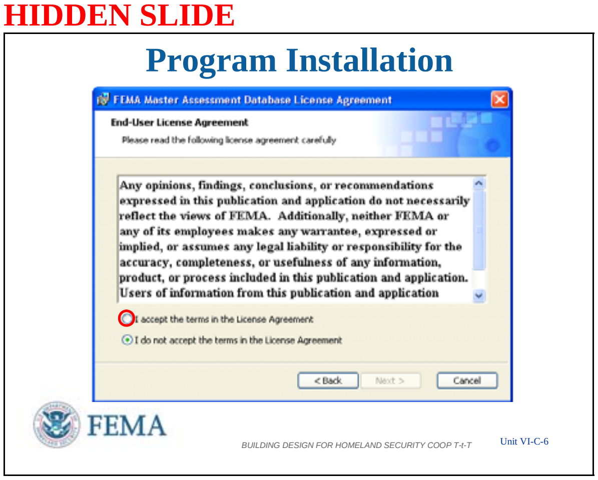
VISUAL VI-C-5
HIDDEN SLIDE

Program Installation

The Install Wizard first identifies the name of the software being installed.

- Left Click on <Next> to continue after confirming that this is the software you want to install.

VISUAL VI-C-6
HIDDEN SLIDE



Program Installation – EULA (1 of 2)

Again, a standard screen showing the End User License Agreement (EULA).

Read as you feel appropriate.

- Left Click on <Accept> circle to continue.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-7
HIDDEN SLIDE

Program Installation – EULA (2 of 2)

- Left Click on <Next> to continue the installation.

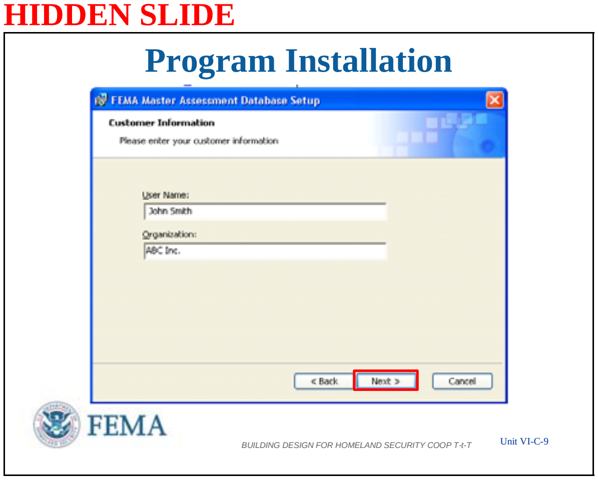
VISUAL VI-C-8
HIDDEN SLIDE

Program Installation – Customer Information (1 of 2)

Then customer information comes up.

Add User Name and Organization in the appropriate windows.

VISUAL VI-C-9
HIDDEN SLIDE



Program Installation – Customer Information (2 of 2)

Once the User Name and Organization have been added, continue with the installation by:

- Left Click on <Next>

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-10
HIDDEN SLIDE

Program Installation – Typical Installation

There is no advantage in using the Custom Installation. There are no component programs to select. The only feature that the Custom Installation allows is to change the file name and/or file location which can result in an excessive path length that aborts the installation.

It is recommended to follow the Typical Installation.

NOTE to instructor: Typical Installation is also recommended as then all folders and files will be where they are expected to be for students to follow along.

- Left Click on <Typical>

VISUAL VI-C-11
HIDDEN SLIDE

Program Installation – Ready to Install

Another standard screen to ensure you are ready to install.

- Left Click on <Install>

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

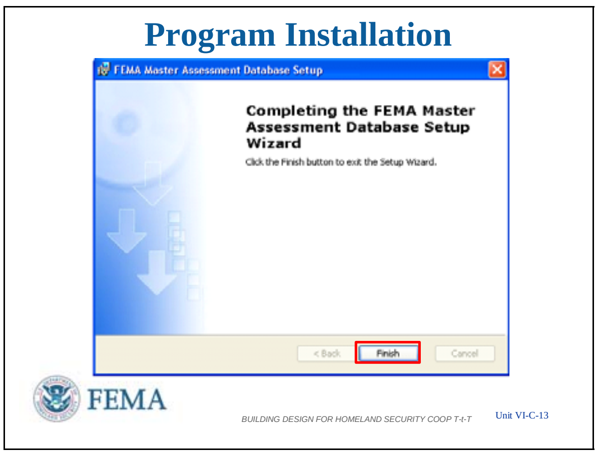
VISUAL VI-C-12
HIDDEN SLIDE

Program Installation – Completion (1 of 2)

If the Access program is not located in the standard location, the Install Wizard will take a long time looking for it with a searching flashlight. It should eventually find it and get to this setup screen.

The timeline will indicate the progress of the installation and eventually reach completion.

VISUAL VI-C-13
HIDDEN SLIDE

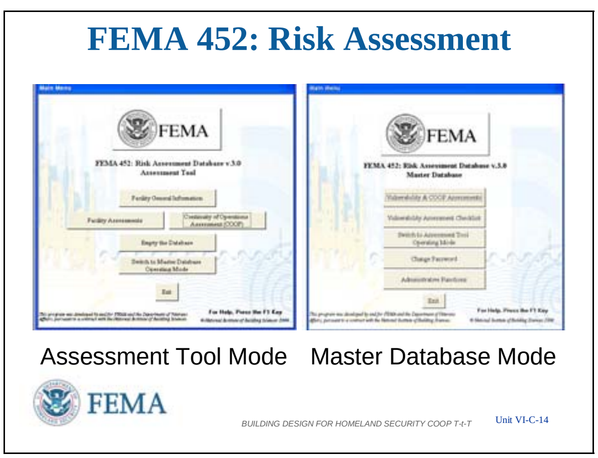


Program Installation – Completion (2 of 2)

The final screen indicates the Install Wizard has completed the installation.

- Left Click on <Finish> to complete the installation.

VISUAL VI-C-14

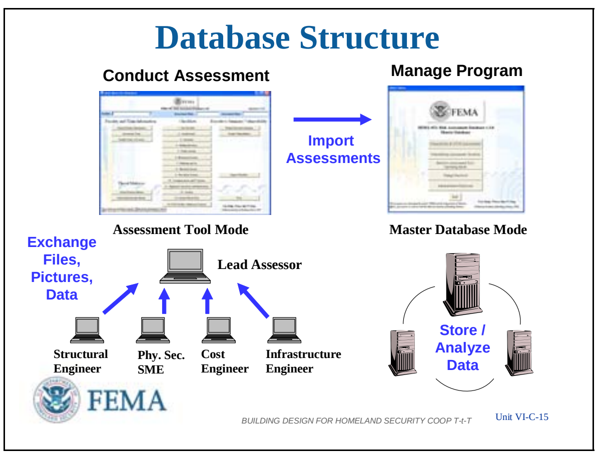


Database Overview (1 of 2)
NOTE to instructor: If installation slides were shown tell students to shift their attention to the screen at the front of the room. Otherwise ignore this note.

- The first thing to understand is that an organization will generally use two different copies of the database: one loaded on a laptop and operating in the Assessment Tool mode for conducting assessments in the field, and the other loaded on a computer at your organization's headquarters and operating in the Master Database mode for collecting the results from the assessors, printing reports, and archiving the results from a number of assessments. The Master Database copy also provides the organization the ability to search for vulnerabilities common to many assessed facilities, search for specific vulnerabilities, etc. Essentially it can be used as a Risk Management tool to identify and track mitigation measures to reduce risk.

- The Assessment Tool mode was designed for engineers and security specialists to be able to easily collect data from the facility being assessed. The Master Database mode was designed for the Program Manager. As you will see, the software is very user friendly.

VISUAL VI-C-15



NOTE to instructor: Loading database information can be done by a Program Manager before the assessment or by an Assessor during the assessment for Versions 2.0 and 3.0. It has to be done by a Database Manager in Version 1.0.

Database Overview (2 of 2)

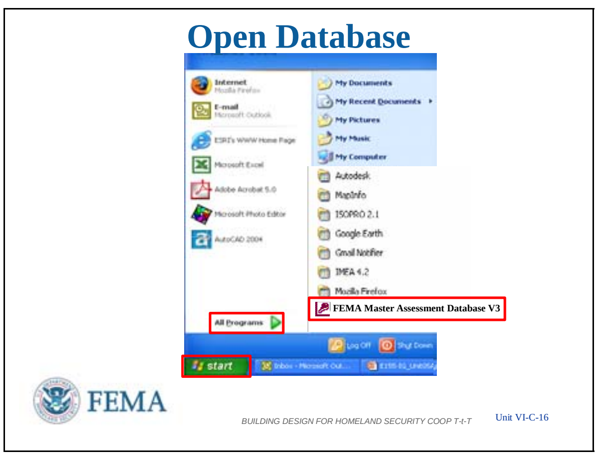
This diagram shows how the two copies of the database interact. When an organization collects information and prepares to conduct an assessment of a facility or a series of facilities, an Assessment Tool database can be prepared. Into this Assessment Tool is placed references, site plans, GIS portfolios, and other facility specific data that is known about the assessment facility or is developed during the pre-assessment phase. Loading this information can be done by a Project Manager before the assessment and then imported into the Assessment Tool database or the information can be loaded by an assessor during the assessment.

This Assessment Tool database is then given to the assessment team and is loaded on one or more assessment computers (usually laptop computers). Either a database containing only the facilities to be assessed

INSTRUCTOR NOTES	CONTENT/ACTIVITY

can be linked to the Assessment Tool or it can be imported into the Assessment Tool database already on the laptop. The assessment team then conducts the assessment and records information and adds collected files using the Assessment Tool operating mode. At the end of the assessment, the assessment team leader uses the Import Checklist function in the Assessment Tool operating mode to combine the team's checklist, vulnerability and recommendation entries into one record. They also manually combine photos, GIS portfolio, and miscellaneous files into the lead assessor's database folder. The Project Manager then uses the Import Assessor Database function in the Master Database operating mode to transfer the complete assessment data and files into the Master Database for analysis and printing.

VISUAL VI-C-16



Open Assessment Tool

Now go to your computers to follow the access procedures to get into the database.

To open the database:

- Left Click on <Start>
- Left Click on <Programs>

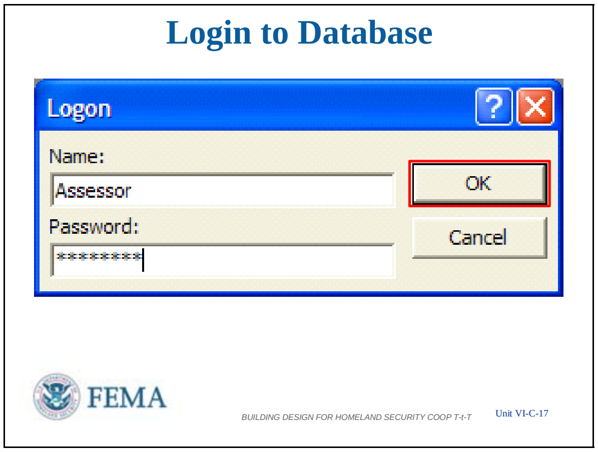
And look for the <FEMA Master Assessment Database >

- The FEMA Master Assessment Database will be at the end of the Startup Program Menu after completing the installation.
- Left Click on <FEMA Master Assessment Database > to enter the database

You can move the shortcut for the FEMA Master Assessment Database to another location within the Startup Menu at any time, such as in alphabetical order. Simply drag and drop.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-17



Open Assessment Tool -- Login

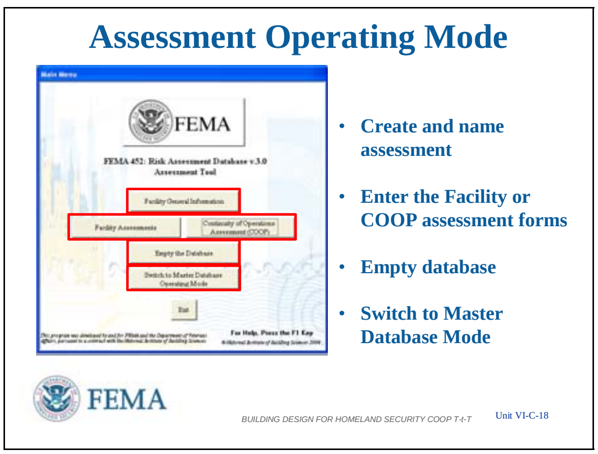
The next action to enter the database is the Logon. You can enter the database as an Assessor, Editor, Reader, or Administrator.

If you enter the new database with the user name of "Assessor", the initial Password is "Assessor". Type "Assessor" as the password matching the capitalization.

Each user can change their password. A user with "Admins" permission (Admins User Group, such as Database Manager or Database Administrator) is needed to create new user accounts.

- Left Click on <OK> to continue

VISUAL VI-C-18



Open Assessment Tool – Assessment Tool Operating Mode

You should be at the main page of the Assessment Tool operating mode in Version 3. It is not found in Version 1 which goes directly to the Assessment screen.

Left Click to advance the slide bullets as you brief.

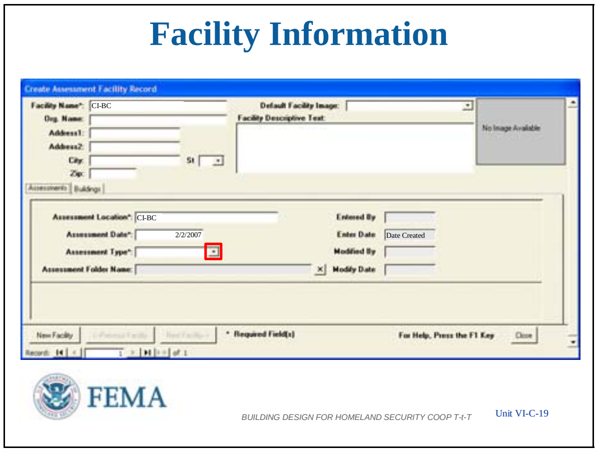
- The first action is to characterize the site assessment in the Assessment Tool by Left Clicking on <Facility General Information> and creating a new site. Any Assessor can create a site.
  [Left Click to advance slide bullets.]
- If the Facility Information has already been loaded, you can go directly to an assessment screen by Left Clicking on <Facility Assessments> or <Continuity of Operations Assessments (COOP).
  [Left Click to advance slide bullets.]
- Assessor laptops may have limited storage capacity and can become bogged down by

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	continuing to store many assessments. The <Empty Database> feature allows clearing of the database (with multiple requests for confirmation). Copy the database and all other collected information to a CD before emptying. Assessors may find it beneficial to refer to similar entries from previous assessments, especially the recommended mitigation measures for similar vulnerabilities. To save time recommend using a consistent filing / naming system to find past assessments. o **Note**: <Empty Database> **cleans** Site Information, Team Members, Points of Contact, Observations, Recommendations, Vulnerabilities, Status, Costs, and the Executive Summary for ALL sites in the Assessment Tool database. o However, it does **NOT** empty the GIS Portfolio, Miscellaneous Files, and Photos in their separate subfolders, as these are not part of the Microsoft Access database. Thus, these files have to be deleted separately after using the same filing / naming system for recording. [Left Click to advance slide bullets.] • The <Switch to Master Database Operating Mode> button takes you to the Master Database features and allows the Assessor to use the reports feature to check the final appearance of the information entered, to identify and prevent duplicate entries, and to easily review the information rather than having to scroll through the Assessment Tool database. [Left Click to advance slide] First time entering the database (with no prior assessments entered): Left Click <General Facility Information> and the software will immediately go to the

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

<Create Assessment > input screen.

VISUAL VI-C-19



Assessment Tool – Facility Information (1 of 3)

In this screen, the “Create Facility Assessment Record,” we will create a new site in Facility General Information.

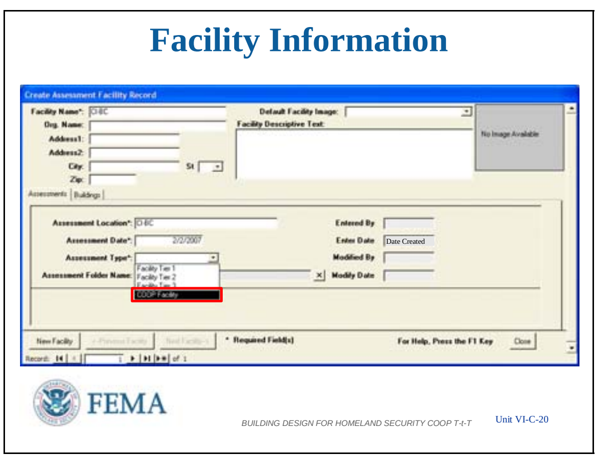
<u>If assessments have already been entered</u>, then a new assessment can be created by Left Clicking on the <New Facility> button in the lower left corner.

Note the asterisked (*) entries that are the minimum required to create an assessment: Facility Name, Assessment Location, Assessment Date, and Assessment Type.

Facility Name, Assessment Location, and Assessment Date are self explanatory.

NOTE: Facility Name and Assessment Location should not have any characters restricted by Microsoft for use in file names. This is due to the automatic generation of folders in Program Files using these entries.

VISUAL VI-C-20



Assessment Tool – Facility Information (2 of 3)

However, Assessment Type needs some clarification. Refer to FEMA 452, Page 3-2, for information on Assessment Type / Level of Assessment for the explanation of Tier 1, Tier 2, and Tier 3.

[See “**NOTE** to instructor” in the left column under the slide for Tier information.]

When an assessment is designated as a “COOP Assessment”, this prompts the system to display additional tabs /menus / forms to further characterize the COOP facility. I’ll show these forms on upcoming slides.

NOTE to instructor: Assessment Type / Level of Assessment

1. **Tier 1.** A Tier 1 assessment is a

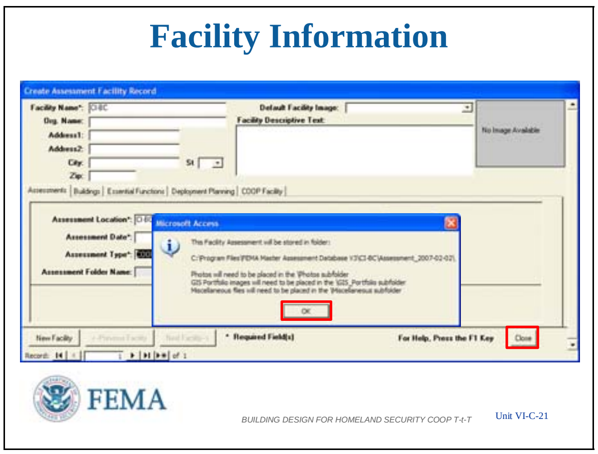
INSTRUCTOR NOTES	**CONTENT/ACTIVITY**
screening phase that identifies the primary vulnerabilities and mitigation options, and is a "70 percent" assessment (see Table 3-1). A Tier 1 assessment can typically be conducted by one or two experienced assessment professionals in approximately 2 days with the building owner and key staff; it involves a "quick look" at the site perimeter, building, core functions, infrastructure, drawings, and plans. A Tier 1 assessment will likely be sufficient for the majority of commercial buildings and other noncritical facilities and infrastructure. 2. **Tier 2.** A Tier 2 assessment is a full on-site evaluation by assessment specialists that provides a robust evaluation of system interdependencies, vulnerabilities, and mitigation options; it is a "90 percent" assessment solution (see Table 3-2). A Tier 2 assessment typically requires three to five assessment specialists, can be completed in 3 to 5 days, and requires significant key building staff participation (e.g., providing access to all site and building areas, systems, and infrastructure) and an in-depth review of building design documents, drawings, and plans. A Tier 2 assessment is likely to be sufficient for most high-risk buildings such as iconic commercial buildings, government facilities, schools, hospitals, and other designated high value infrastructure assets. 3. **Tier 3.** A Tier 3 assessment is a detailed evaluation of the building using blast and weapons of mass destruction (WMD) models to determine building response, survivability, and recovery, and the development of mitigation options. A Tier 3 assessment (see Table 3-3) typically involves engineering and scientific experts and requires detailed	• Left Click on **COOP** as the **Assessment Type**.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

design information, including drawings and other building information. Modeling and analysis can often take several days or weeks and is typically performed for high value and critical infrastructure assets. The Assessment Team is not defined for this tier; however, it could be composed of 8 to 12 people.

COOP Facility: The COOP Facility assessment designation is used to designate an assessment of a COOP facility.

VISUAL VI-C-21



Assessment Tool – Facility Information (3 of 3)

When data input is complete:

- Left Click <Close> to create the Assessment Site.

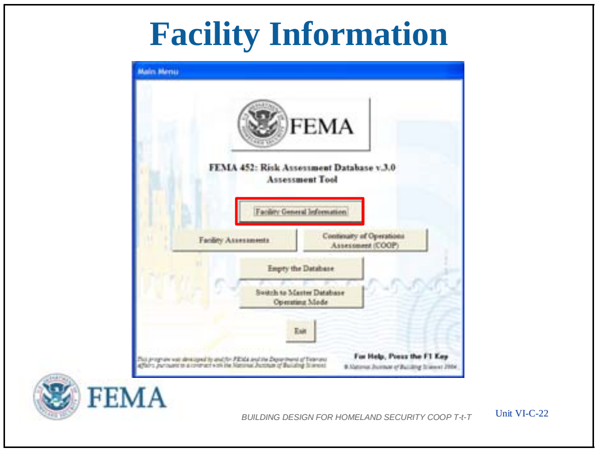
When you create the site, the software automatically creates subfolders named GIS Portfolio, Miscellaneous Files, and Photos, all under a main folder that uses the assessment location and assessment date as the main folder name. If you changed the program location using Custom Installation, then you should make note of the file path that these subfolders are placed in, as you will need that information to properly load and link the contents of these subfolders to the Assessment Tool database.

- Left Click <OK> to finish creating the Assessment Site.

NOTE to instructor: This may be a good place to use a laser pointer to show these entries as they are being mentioned.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-22

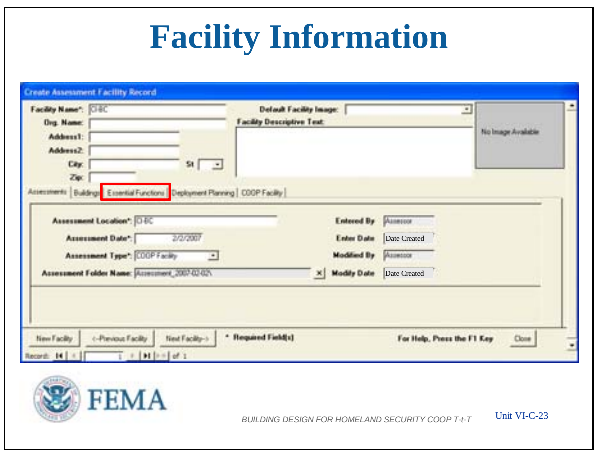


Assessment Tool – COOP Facility Information (1 of 3)

After hitting <Close> when loading Facility Information the software kicks back to the main menu. If <Close> is not pressed, but the cursor is Left Clicked anywhere else on the screen will allow entry into the additional COOP Facility information screens.

Reenter <Facility General Information> to get to the COOP Facility information just entered.

VISUAL VI-C-23



Assessment Tool – COOP Facility Information (2a of 3)

When an assessment is designated as a "COOP Assessment," this prompts the system to display Checklist #14 on the Assessment Tool main menu as you will see later and also adds the following three tabs to this form:

- Essential Functions
- Deployment Planning
- COOP Facility

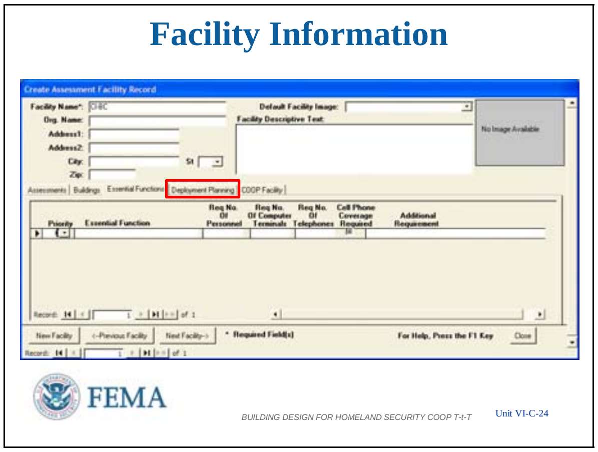
Use these three tabs to record COOP related information on the facility.

These tabs contain the information you were given in Unit 1 of your Student Manual as taken from the Appendix C Case Study.

You can refer to this facility information during the assessment process.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

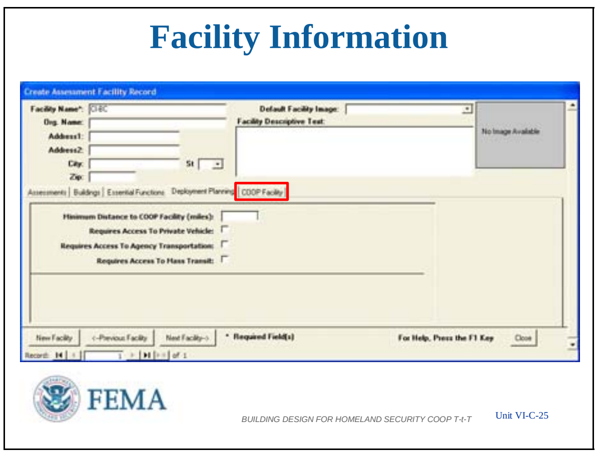
VISUAL VI-C-24



Assessment Tool – COOP Facility Information (2b of 3)

Essential Functions information loads in a manner like loading a Point of Contact.

VISUAL VI-C-25



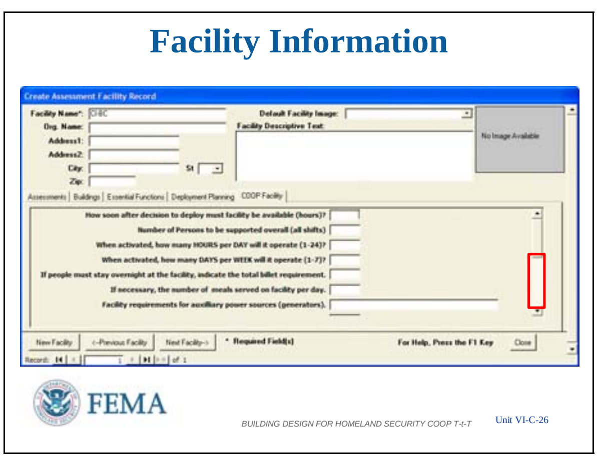
Assessment Tool – COOP Facility Information (2c of 3)

Deployment Planning covers that information which the Alternate Facility should be assessed against for COOP requirements.

Enter the miles that policy states that the COOP facility must be from the Primary Facility.

Check the other boxes if the answer is “Yes”

VISUAL VI-C-26



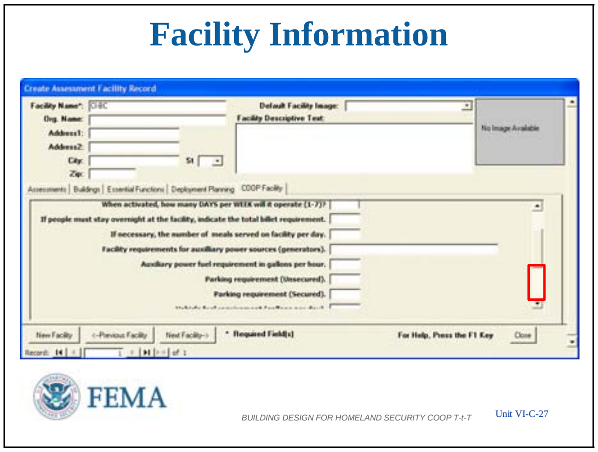
Assessment Tool – COOP Facility Information (2d of 3)

COOP Facility Information does not fit on one screen so the vertical scroll bar is available to access this information.

Left Click in the open area of the scroll bar shown by the red box to see the next blocks for information input.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-27

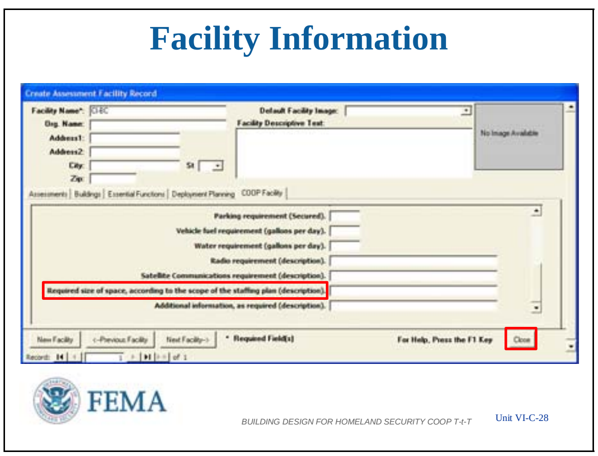


Assessment Tool – COOP Facility Information (2e of 3)

Then Left Click in the open area of the scroll bar shown by the red box to see the final information input blocks.

Again note that this is the same information covered in the Unit 1 Student Activity.

VISUAL VI-C-28



Assessment Tool – COOP Facility Information (2e of 3)

- Left Click – illustrate [red box] space requirements

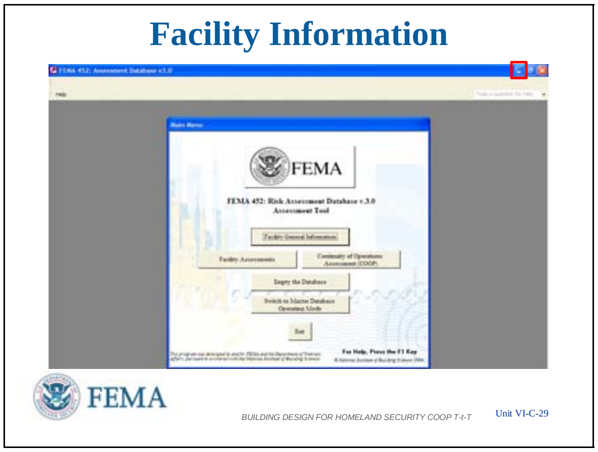
This was your square footage and workstation space requirements exercise in Unit 1

- Left Click – remove illustration [red box]

- Left Click <Close> to go to the next demonstration.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL VI-C-29



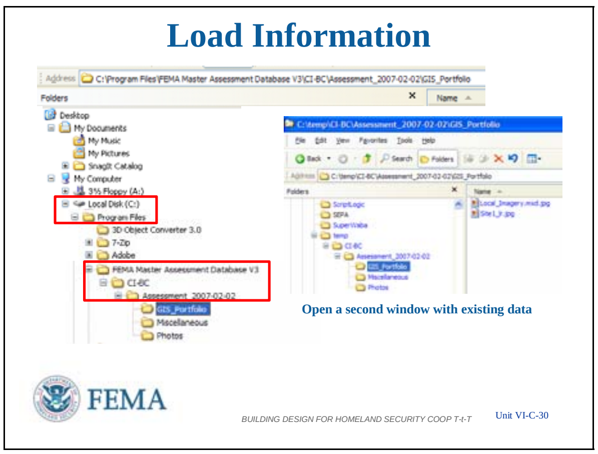
Assessment Tool – COOP Facility Information (3 of 3)

Closing the previous screen takes us back to the Main Menu.

To continue the next demonstration:

- Left Click on <Reduce> button in the upper right corner as our next actions are outside of the database.

VISUAL VI-C-30



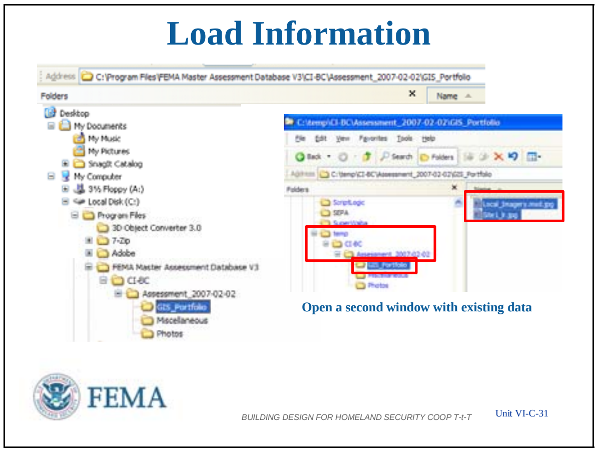
Assessment Tool – Load Added Files (1 of 4)

Let's look at the process to load the information into the newly created subfolders when we created the Facility Assessment Site information.

- First open My Computer or Windows Explorer to find those storage locations (folders) created by the Facility General Information creation process.
  - Folder names must match Assessment Location and Date to ensure future linkages for loading
- Next, open another window in My Computer or Windows Explorer to find the information collected either before or during the assessment.
  - **NOTE**: For student convenience, the Database CD contains subfolders that have the files shown in these slides to illustrate the transfer process.
- This example shows two GIS Images to transfer.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-31

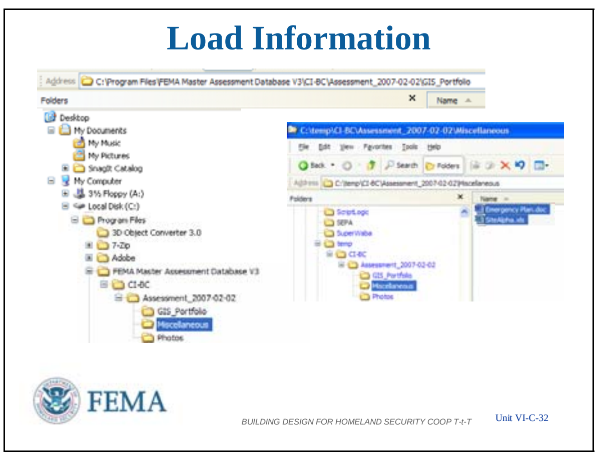


Assessment Tool – Load Added Files (2 of 4)

A Drag-and-Drop operation is shown to transfer the files to the necessary subfolders to later link with the database.

- To ensure copying depress <Ctrl> to get the small plus sign in a box, otherwise the files will be moved.
- You can also <Right Click> on the collected files, copy them by Left Clicking <Copy> in the pull down menu, and then move to the necessary subfolders, <Right Click> on the appropriate folder, then paste by Left Clicking <Paste> in the pull down menu.
- Just ensure that all files are transferred – either copied or moved into the necessary subfolder with the GIS Portfolio being shown here. Copying is recommended just in case anything unforeseen occurs.

VISUAL VI-C-32



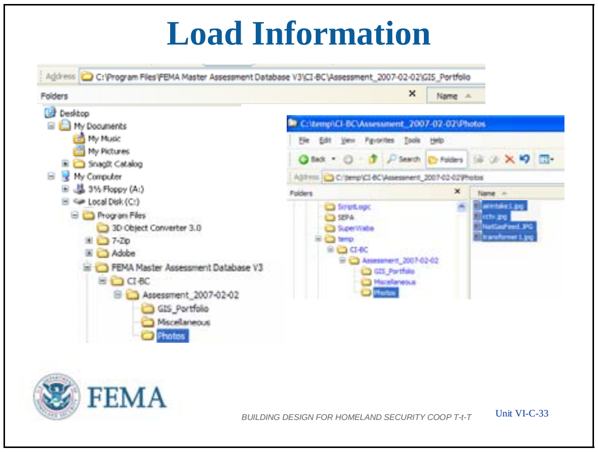
Assessment Tool – Load Added Files (3 of 4)

The same Drag-and-Drop operation between the two windows allows copying of the files contained in the folder marked Miscellaneous.

Two files to be passed between the two Miscellaneous folders.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

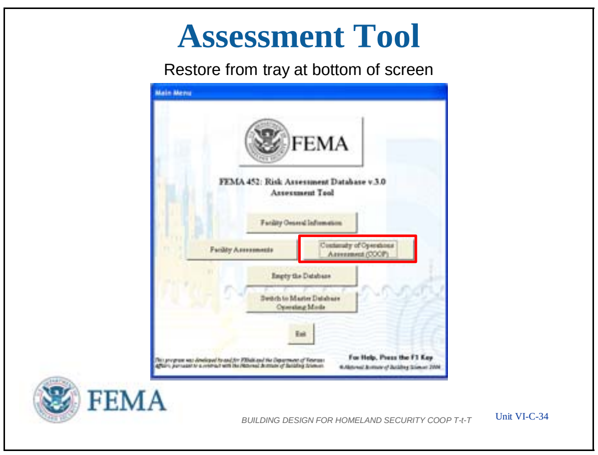
VISUAL VI-C-33



Assessment Tool – Load Added Files (4 of 4)

Copy the four photos between the two Photos folders.

VISUAL VI-C-34



Assessment Tool – Team Members (1 of 4)

After demonstrating the movement of GIS Portfolio, Miscellaneous, and Photos files, we need to get back to the Assessment Tool Main Menu.

Restore the main menu screen by Left Clicking on the tab for the program in the tray at the bottom left of the screen to the right of the Start button.

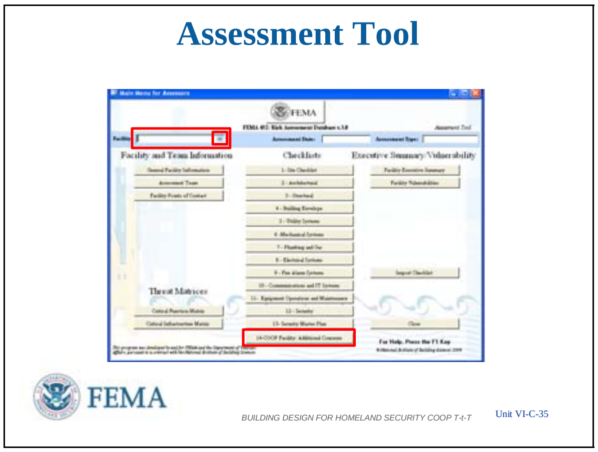
From the Assessment Tool Main Menu:

- Left Clicking on <Facility Assessments> or <Continuity of Operations Assessment (COOP)> to enter the Main Menu for Assessors.
  - The link to <Facility Assessments> provides access to Facility Tier 1 to Facility Tier 3 assessments and the standard 13 checklists.
  - The <Continuity of Operations Assessment (COOP)> link provides access to COOP assessments, the standard 13 checklists <u>and</u> the 14th checklist titled "COOP Facility: Additional concerns."
  - Both forms function in the same

manner.

- Left Click on <Continuity of Operations Assessment (COOP)> to continue investigating the database.

VISUAL VI-C-35



Assessment Tool – Team Members (2 of 4)

Since we entered through the COOP Assessment button on the previous screen we will find the Checklist #14 COOP Facilities.

- Left Click for red box around Checklist #14.
- Left Click to remove red box.

Once in the Main Menu for Assessors, the first action on this screen is to choose an assessment facility, since several may be loaded.

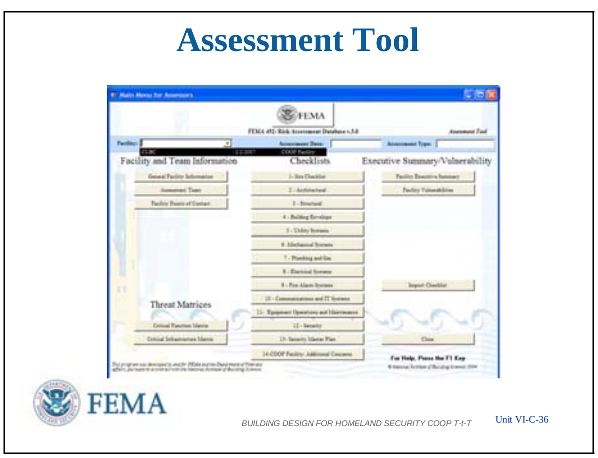
- Left Click for red box around Facility window.
- Left Click to remove red box.

To select an assessment:

- Left Click on <u>down arrow in the “Facility:” window</u>.

This will display the pull-down list of available assessments.

VISUAL VI-C-36



Assessment Tool – Team Members (3 of 4)

You put CI-BC into a <u>new</u> database so CI-BC is the only assessment you will find.

Once an assessment facility has been chosen, the assessor can go into any of the data entry buttons:

- Assessment Team
- Facility Points of Contact
- Threat Matrices
- Checklists
- Executive Summary

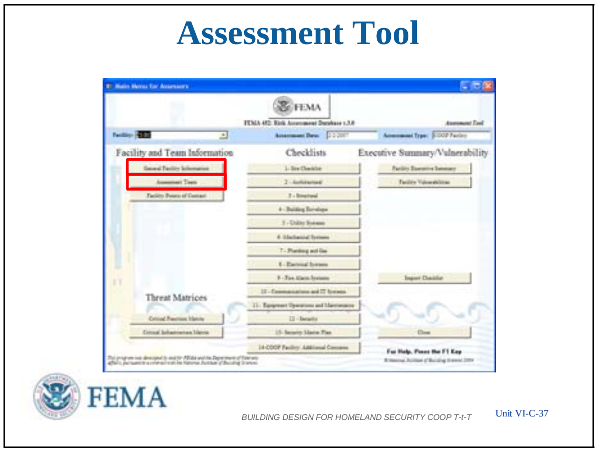
OR

- Facility Vulnerabilities

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

- Left Click on CI-BC to select that assessment.

VISUAL VI-C-37



Assessment Tool – Team Members (4 of 4)

Now CI-BC shows in the Facility window as well as the date and assessment type in the other two windows. These three bits of information uniquely describe this assessment in the database.

- Left Click for red box around General Facility Information button.

NOTE: If you go into General Facility Information <u>with an assessment selected</u> you will get a Facility Information Report, not a data entry screen. This is to prevent changing anything at this level since it affects files already named. If you want to input information into General Facility Information you must go back to the Main Menu and enter that way. However, do not think of changing any * (asterisked) entries as these name file folders already created and changing the name will not change those folder names.

- Left Click to remove red box.

- Left Click on <Assessment Team> to continue data entry.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-38

Add Team Members (1 of 4)

The Assessment Team tab takes you to the fill-in-the-blank lists for keeping track of Team Members.

- Left Click on <Add New Team Member> to access the input screen.

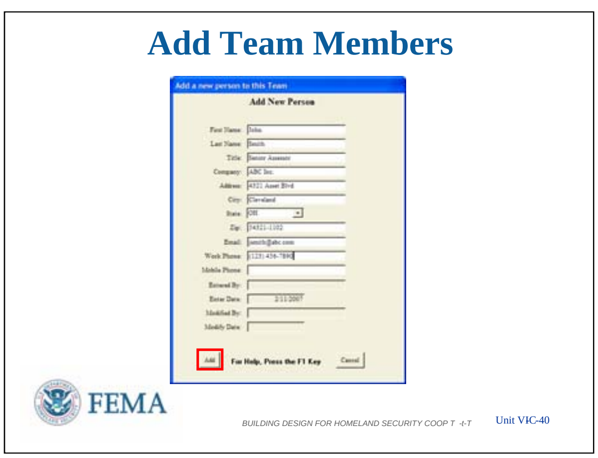
VISUAL VI-C-39

Add Team Members (2 of 4)

However, like most software, there is a confirmation step.

- Left Click on <Yes> to continue.

VISUAL VI-C-40



Add Team Members (3 of 4)

Fill in this screen with as much information as is available or desired.

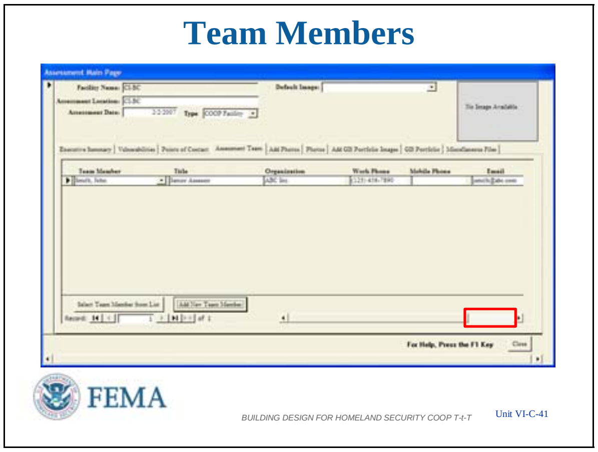
<u>Minimum information</u> required to add a team member:

- First Name
- Last Name
- City
- State

- Left Click on <Add> button to place this team member in the database.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-41

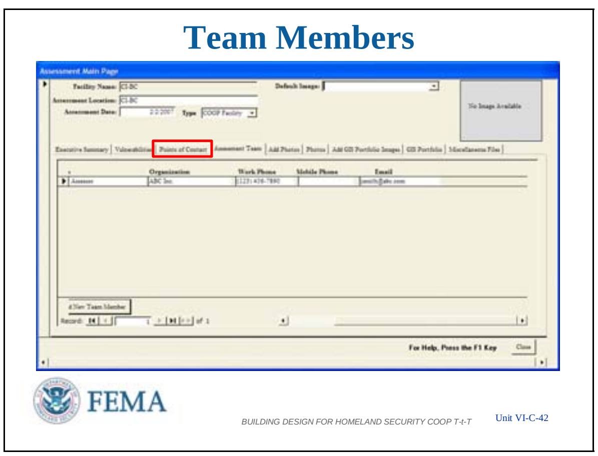


Add Team Members (4 of 4)

After adding the Team Member, you are taken back to the Team Members List and you can see the information entered.

- Use the scroll bar or direction arrows in the lower right to see the remaining information.
  NOTE: In Version 4.0, the scroll bar provides access to all the Team Member information.
- The other buttons allow you to select the Team Member from a List or remove the Team Member from this assessment.
- At this point you can Left Click on <Close> to go back to the Assessments screen or you can continue loading information using the tabs in the middle of the screen.

VISUAL VI-C-42



Assessment Tool – Points of Contact (1 of 3)

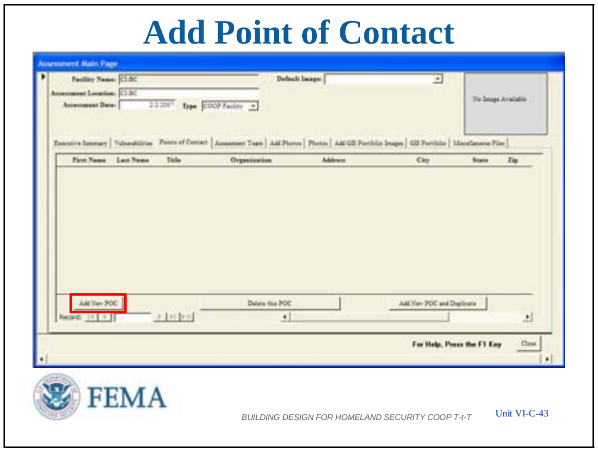
- Left Click for red box around Points of Contact

The Points of Contact tab takes the Assessor to the Points of Contact screen for keeping track of the people to be contacted during the assessment or that were identified and met during the assessment.

- Let us now go to the <Points of Contact> by Left Clicking the tab.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-43

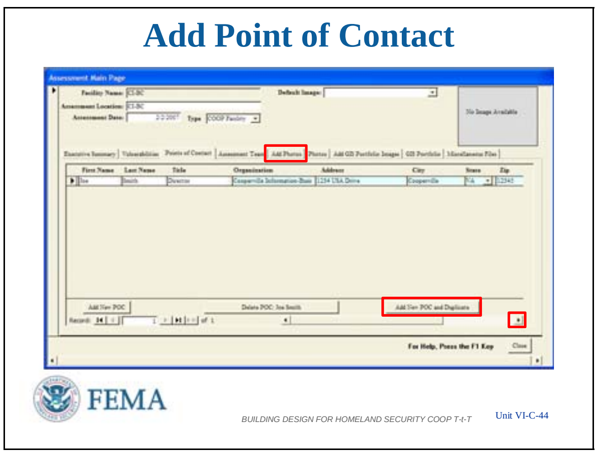


Assessment Tool – Points of Contact (2 of 3)

The buttons across the bottom allow you to add or delete Points of Contact as needed.

- Left Click on <Add New POC>

VISUAL VI-C-44



Assessment Tool – Points of Contact (3 of 3)

This input screen is different than the Team Members input screen as you enter the information directly in each cell. You can enter the information and move to the next cell by using the <Tab> feature on the keyboard or by Left Clicking on the Cell directly.

- Use the scroll bar or arrow in the lower right to move the screen to see the remaining information on the POC line.
- Then you must press <Enter> after the cells are complete to add the information to the database.
- There's even a feature in the POC list to <u>duplicate</u> the information from previous entries (light blue shaded cells).
  - o Left Click the left column to get the right arrow on the entry to indicate the selection to duplicate.
  - o Left Click on <Add New POC and Duplicate> button
  - o The light blue blocks will be duplicated on the next entry line.
  - o This is useful because it is likely that many, if not all, of the POC's will

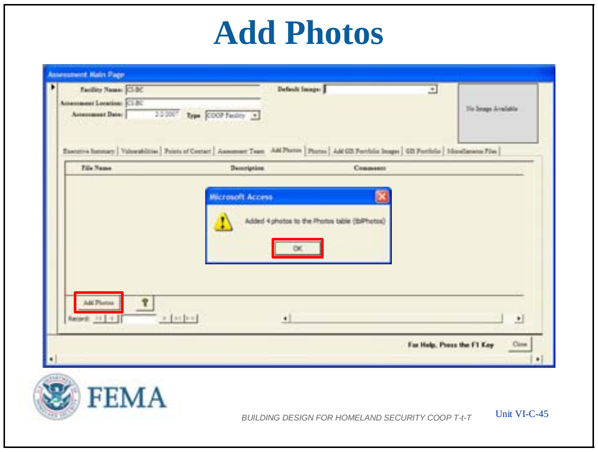
INSTRUCTOR NOTES	CONTENT/ACTIVITY

share the same business address.

Continuing with the data entries, we next go to Adding Photos

- Left Click on <Add Photos> tab in the center of the screen.

VISUAL VI-C-45



Assessment Tool – Link and Load Added Files – Photos (1 of 6)

Even though we have placed the GIS Portfolio, Miscellaneous Files, and Photos into the proper subfolders, we must still link them to the database in a two step process.

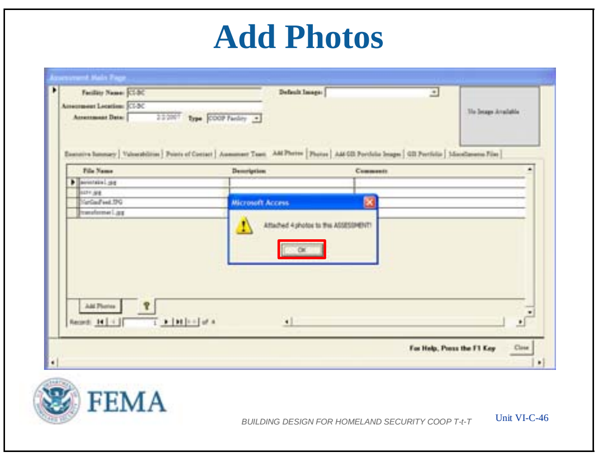
In the Add Photos screen:

- Left Click on <Add Photos> button in the lower left to perform the first step.

The first pop-up confirms that the files were added to the table in the database

- Left Click on <OK> to continue with the process

VISUAL VI-C-46



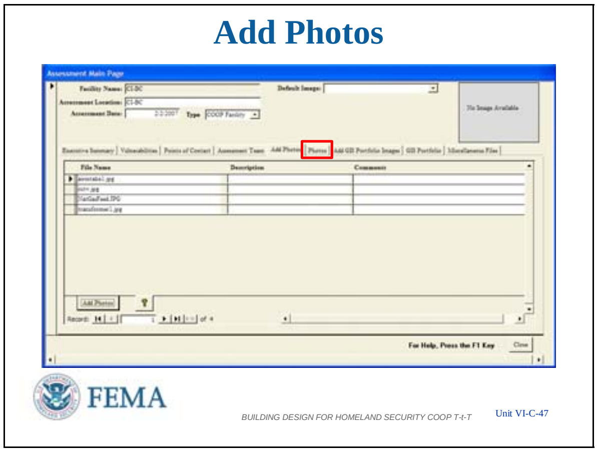
Assessment Tool – Link and Load Added Files – Photos (2 of 6)

Another confirmation that 4 photos are attached as well as indicated in the list shown. The photos can have descriptions and comments added here.

- Left Click on <OK> to continue with the process

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

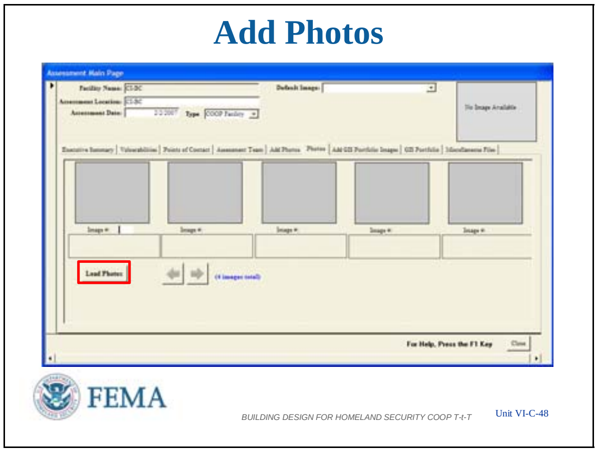
VISUAL VI-C-47



Assessment Tool – Link and Load Added Files – Photos (3 of 6)

- Left Click on <Photos> tab to continue with the loading process.

VISUAL VI-C-48



Assessment Tool – Link and Load Added Files – Photos (4 of 6)

Now in the Photos screen:

- Left Click on <Load Photos> in the lower left corner

This makes the linked photos visible within the Assessment Tool.

NOTE to instructor: An error pop-up window has occurred in this screen as follows:

> FEMA 452: Assessment Database v3.0 doesn't support the format of the file C:\Program files\FEMA Master Assessment Database V3\CI-BC\Assessment-2007-02-02\Photos\Airintake.jpg or file is too large. Try converting the file to BMP or GIF format.
>
> -- This file is the one provided to the students and was successfully loaded by most of the students in the class that this error window was first noticed.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

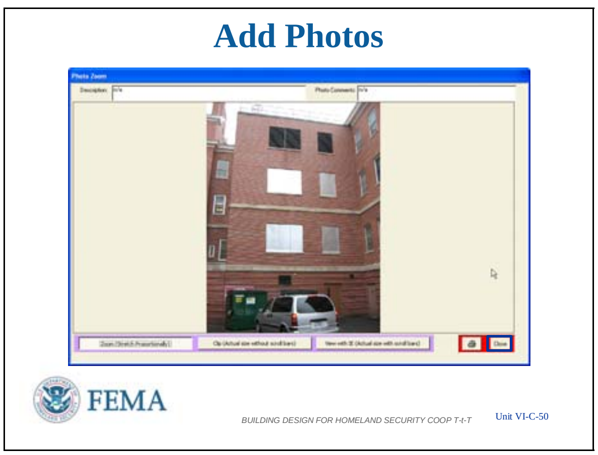
VISUAL VI-C-49

Assessment Tool – Link and Load Added Files – Photos (5 of 6)

Then thumbnails of the photos loaded are shown.

- Left Click on the first photo thumbnail to see additional features

VISUAL VI-C-50



Assessment Tool – Link and Load Added Files – Photos (6 of 6)

After Left Clicking on a photo, a Photo Zoom screen appears which gives a limited capability for viewing the photo in different sizes.

You can Left Click on tabs <Zoom>, <Clip>, or <Internet Explorer> across the bottom of the photo to see the differences.

- When done, Left Click on <Close> to exit.

VISUAL VI-C-51

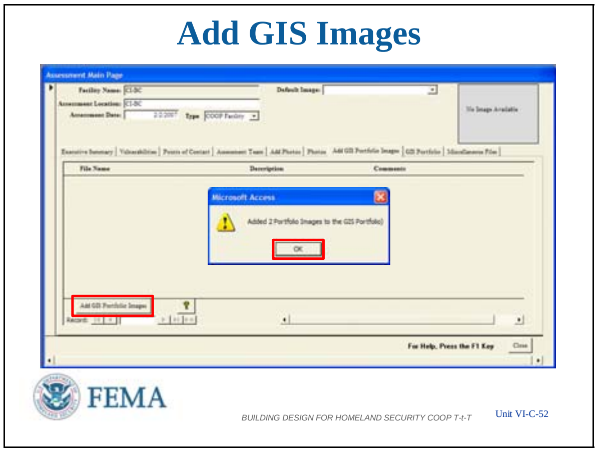
Assessment Tool – Link and Load Added Files – Add GIS Images (1 of 6)

Continuing with the linking of collected data:.

- Left Click on <Add GIS Portfolio Images> tab in the center of the screen.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-52



Assessment Tool – Link and Load Added Files – Add GIS Images (2 of 6)

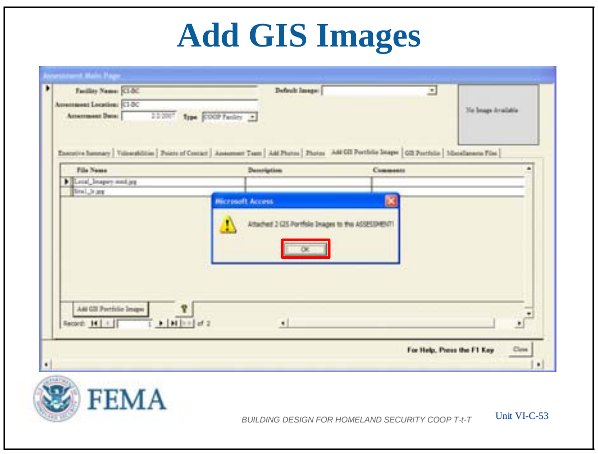
As was done with Photos:

- Left Click on <Add GIS Portfolio Images> in the lower left corner.

And also as with Photos:
The first pop-up confirms that the files were added to the appropriate table in the database

- Left Click on <OK> to continue with the process

VISUAL VI-C-53



Assessment Tool – Link and Load Added Files – Add GIS Images (3 of 6)

Now we see the list of GIS Portfolio Images attached. Note that Description and Comment information can be added on this screen.

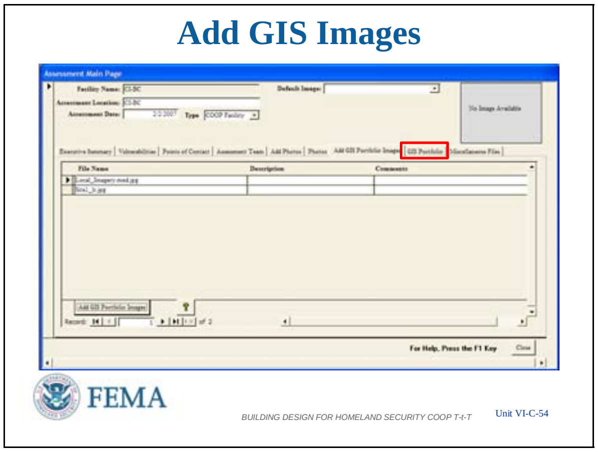
The second pop-up confirms that the images have been attached.

- Left Click on <OK> to continue with the process

INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL VI-C-54

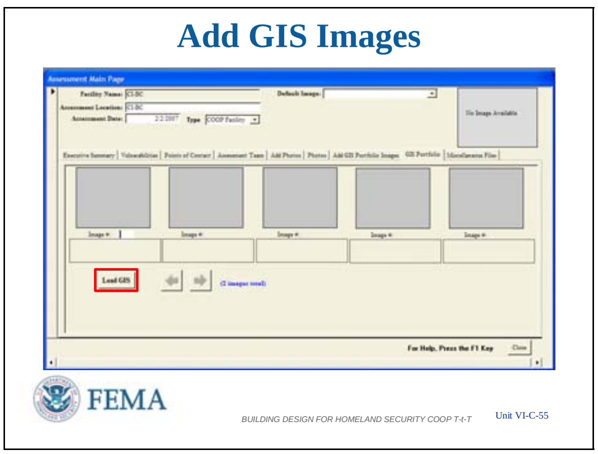


Assessment Tool – Link and Load Added Files – Add GIS Images (4 of 6)

The process is the same as with Photos when loading the GIS Portfolio Images.

- Left Click on <GIS Portfolio> button in the upper right of the screen.

VISUAL VI-C-55



Assessment Tool – Link and Load Added Files – Add GIS Images (5 of 6)

- Left Click on <Load GIS> tab in the lower left corner.

VISUAL VI-C-56

Assessment Tool – Link and Load Added Files – Add GIS Images (6 of 6)

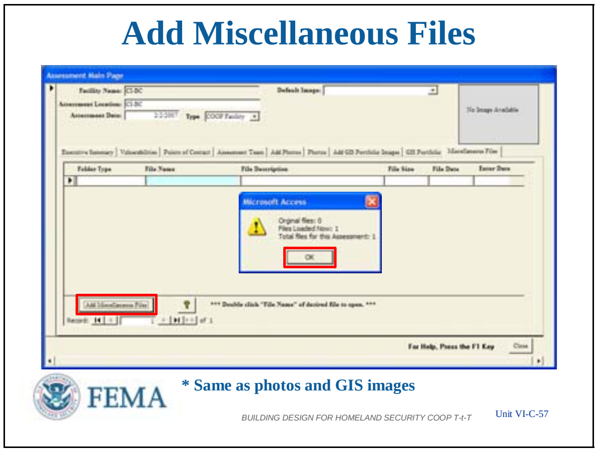
The GIS Images have the same capability as Photos by Left Clicking on the images and seeing them in other sizes.

This completes the GIS Portfolio Images collected data entry process

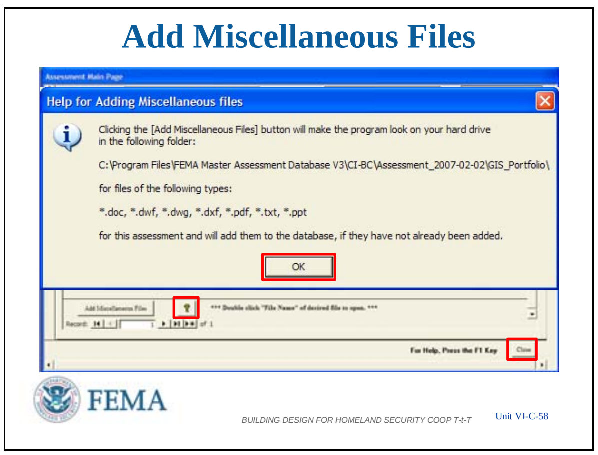
- Left Click on <Miscellaneous Files> tab to perform the last file linkage action.

INSTRUCTOR NOTES

VISUAL VI-C-57



VISUAL VI-C-58



CONTENT/ACTIVITY

Assessment Tool – Link and Load Added Files – Miscellaneous Files (1 of 2)

The process for Miscellaneous files is the same as for Photos and GIS Images.

- Left Click on <Add Miscellaneous Files> to continue linking and loading.

A pop-up indicates that one file was loaded and it shows up in the list.

- Left Click on <OK> to close the pop-up.

However, did we not have two files in the Miscellaneous folder?

Assessment Tool – Link and Load Added Files – Miscellaneous Files (2 of 2)

- Left Click on <Question Mark> to the right of the Add Miscellaneous Files tab.

NOTE to Instructor: This Question Mark is also found on the Photos and GIS Portfolio "Add Files" screens to indicate what file types the database can accommodate.

The Question Mark pops up a screen that shows what files are able to be handled by the software. Our missing file is in .XLS format and that is one of the formats not listed, thus the reason for the linking and loading not occurring.

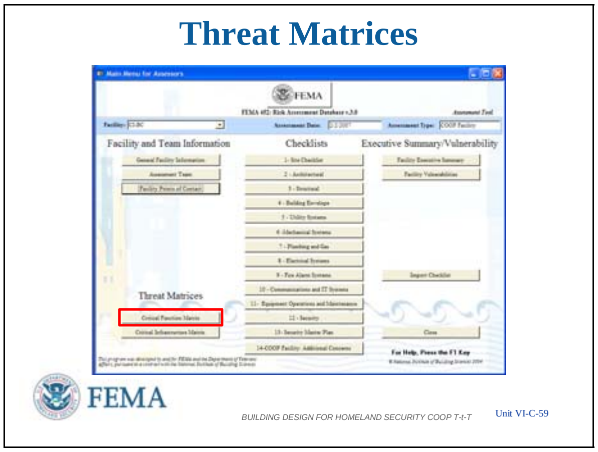
In Version 3.0, Photos and GIS Portfolio images are limited to .JPG format.

In Version 4.0, TIF and .BMP formats for Photos and GIS Portfolio images will be allowed and there will be no restrictions on Miscellaneous files as long as there is software on the computer that can open and read the files.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Left Click on <OK> in the pop-up to continue.
- Left Click on <Close> to go to the next feature.

VISUAL VI-C-59



Assessment Tool – Threat Matrices (1 of 6)

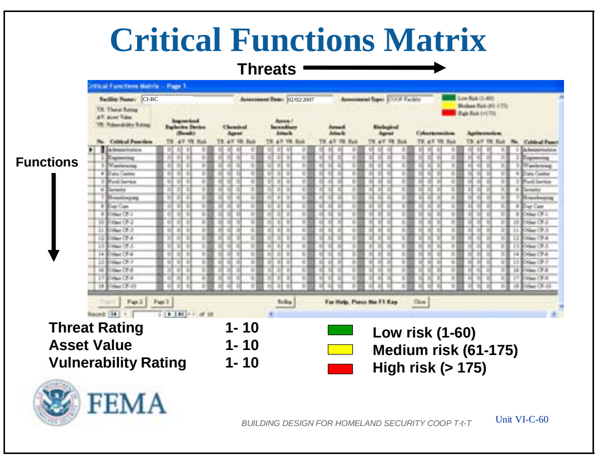
After the available preliminary information is loaded, you can work the Threat Matrices for Critical Functions and Critical Infrastructure. This is an electronic way of collecting the numerical rating information you recorded by hand yesterday.

Ensure you have an assessment facility selected.

In the lower left corner of the Main Menu for Assessors you will find the Threat Matrices buttons.

- Left Click on <Critical Functions Matrix> button in the lower left corner

VISUAL VI-C-60



Assessment Tool – Threat Matrices (2 of 6)

Selecting the <Critical Function Matrix> button will display this screen.

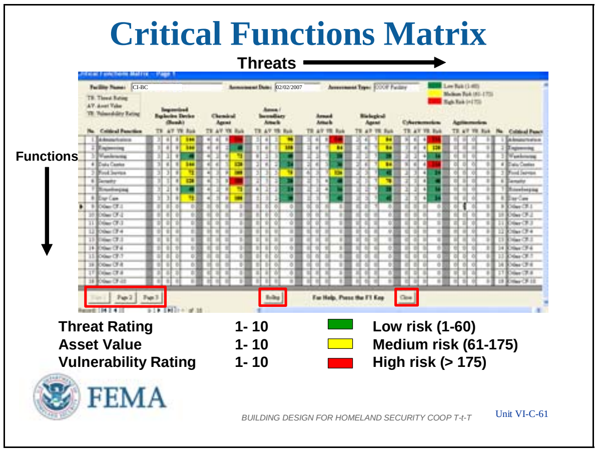
Listed are a range of established threats and functions.

- The matrix allows entry of Threat Rating (TR), Asset Value (AV), and Vulnerability Rating (VR), in horizontal fashion, following the 1 to 10 scale as listed in FEMA 452.
- The Risk Rating is then automatically computed and color coded according to the established scale.

Advance the slide to show how the colors look when data is in the matrix.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-61



NOTE to instructor: Emphasize that the prioritized Essential Functions required for COOP under FPC-65 must be broken down in Critical Functions and Critical Infrastructure to perform a risk assessment. The Essential Functions require specific people to perform the Critical Functions using equipment and utilities identified under Critical Infrastructure. Thus, the "Other #" listings in V3.0 can be inserted directly in V4.0 to facilitate the specific Critical Functions and Critical Infrastructure needed for your COOP Alternate Facility risk assessment.

Assessment Tool – Threat Matrices (3 of 6)

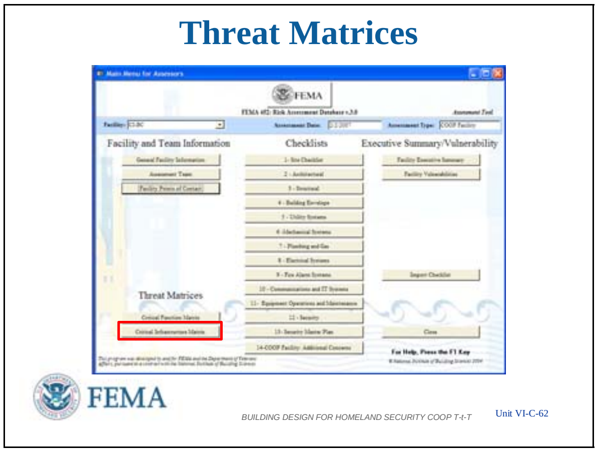
To maintain the FEMA 452 process, the basic Threats and Functions can not be renamed. However, there are unassigned placeholders that can be used to record an organization's unique Critical Functions and Threats. The placeholders for functions are listed under the Critical Function column as "Other CF-1" to "Other CF-10". The threat placeholders are listed across the top of the matrix as "Other 1" and "Other 2." Organizations can designate a meaning for a placeholder, use the placeholder to collect data, then after exporting the matrix to Microsoft Excel©, change the name of the placeholder to a specific threats or function.

NOTE to instructor: In Version 4.0 the Program Manager will be able to adjust the Functions and Threats – adding or deleting as seen fit. Recommend only changing them at the start of an annual assessment cycle with new clean databases to avoid conflicting data in assessments done with different functions and threats. The same holds for infrastructure.

- Selecting the <Page 2> or <Page 3> buttons in the bottom left corner will display additional Threats / Hazards. This is much like shifting the view to the right to see the rest of the matrix.
- Selecting the <Rollup> button displays a consolidated Functions matrix.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-62

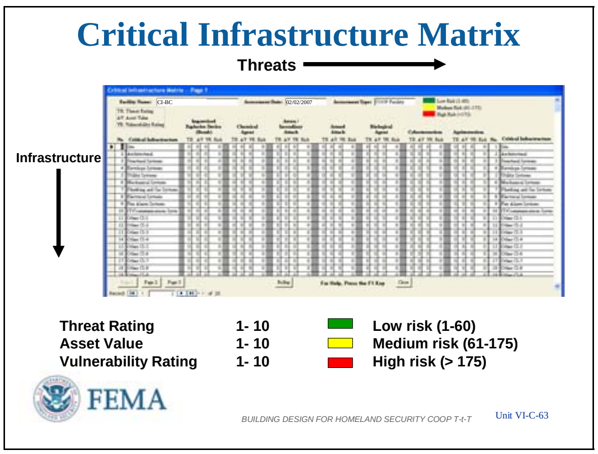


Assessment Tool – Threat Matrices (4 of 6)

The next step is to enter the Critical Infrastructure Threat Matrix to input this information as part of the assessment.

- Left Click on <Critical Infrastructure > button.

VISUAL VI-C-63



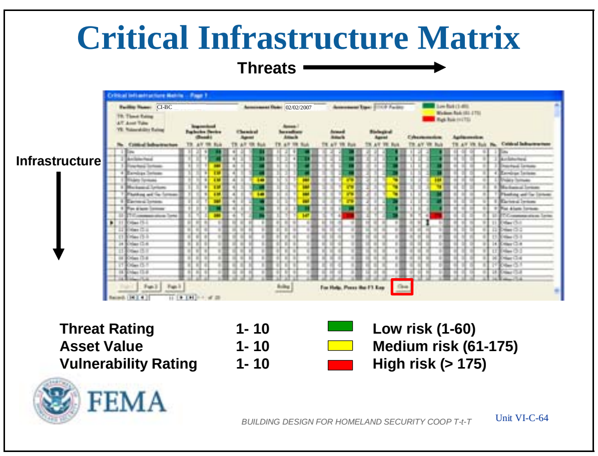
Assessment Tool – Threat Matrices (5 of 6)

As with the Critical Functions Threat Matrix, you get a range of established threats and functions with some "Blank / Unnamed" entries to track specific threats and functions.

Suggest to students to add some numbers for one function and see how the matrix works.

Advance slide by Left Clicking

VISUAL VI-C-64



Assessment Tool – Threat Matrices (6 of 6)

NOTE to instructor: The students will not see this as they have not loaded any information other than the simple entry just done.

The matrix uses the 1 to 10 scale for Asset Value, Threat Rating, and Vulnerability Rating.

The Risk Rating is similarly computed and color coded.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

In the lower left corner of the screen Page 2 and Page 3 work the same way as on the Critical Functions Matrix

Advance slide by Left Clicking

- Students Left Click on <Close> to return to the Main Menu for Assessors screen

VISUAL VI-C-65

Assessment Tool – Checklists (1 of 6)

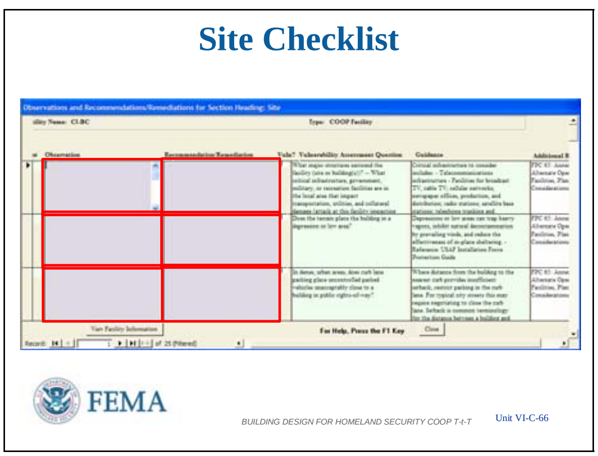
The standard 13 checklists (as in FEMA 426) and the 14th checklist titled "COOP Facility: Additional Concerns", run down the middle of the Main Menu for Assessors screen.

Select an assessment site

- Left Click on <1 – Site Checklist> as an example.

We can then see the format of all checklists within the Assessment Tool.

VISUAL VI-C-66



Assessment Tool – Checklists (2 of 6)

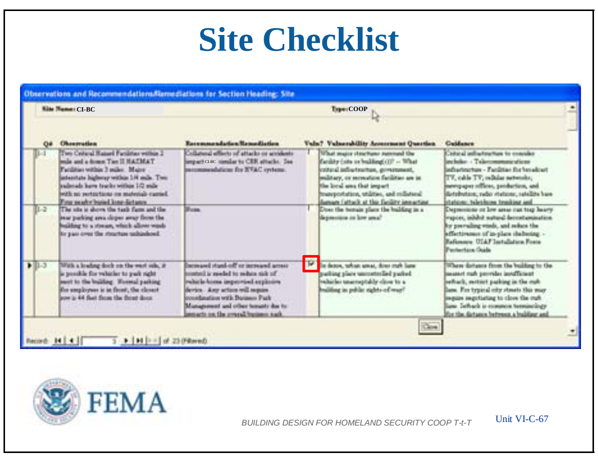
The Site Checklist is like all the other checklists.

- The first column contains an arrow to indicate which row is selected for data entry.
- The second column from the left is the checklist question number [Section Number – Question Number]
- The third column is the Observation made during the assessment. This could describe a vulnerability identified by the Assessor.
    - **Note:** Since reports do not include the original questions to save space, it is prudent to draft your answer so that it includes the question information so that the answer can be understood.
- The fourth column is the Recommendation / Remediation made by the Assessor to

mitigate concerns with this question and observation.
  - **Note**: Similar to Observations, include some understanding of the question when drafting the Recommendation/ Remediation so that it too can stand alone in a report.
- The fifth column is reserved for identifying the questions which have an observation identified as a vulnerability.
- The sixth column is the question itself, taken right from the FEMA 426 Building Vulnerability Assessment Checklist.
- The seventh column is the guidance associated with that question, also found in the FEMA 426 Building Vulnerability Assessment Checklist.
- The eighth column is a cross reference to COOP related guidance.

Left Click to activate the red boxes and highlight each box.
The Observation and Recommendation / Remediation boxes can accept inputs into the database.

VISUAL VI-C-67



Assessment Tool – Checklists (3 of 6)

Left Click to advance the slide.

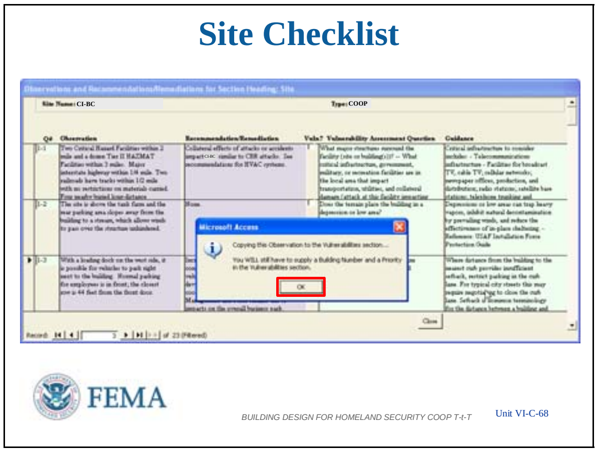
All six boxes (Observation – Recommendation / Remediation) shown are populated with some information

Left Click to reveal a red box around the vulnerability check mark.

- Question 1-3 was identified by the Assessor as a vulnerability to consider. He places a check mark in the box by putting the pointer on the box and Left Clicking.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

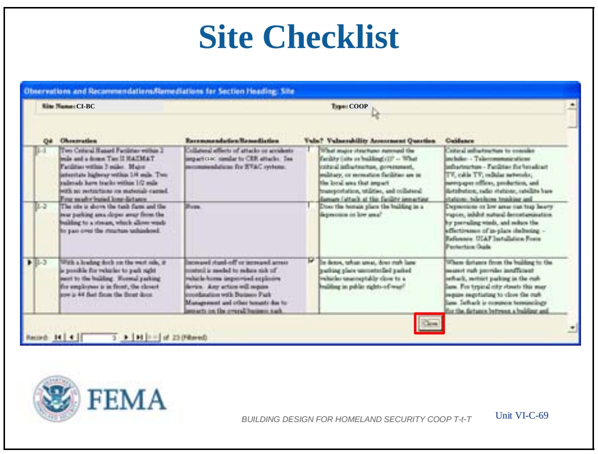
VISUAL VI-C-68



Assessment Tool – Checklists (4 of 6)

- o **Note 1:** The software indicates that more information – building number and priority – will be sought when the Vulnerabilities Screen is opened.
- Left Click on <OK> to close the pop-up window

VISUAL VI-C-69



Assessment Tool – Checklists (5 of 6)

- o **Note 2:** Each time a checkmark is placed in this box, another entry is placed in the Vulnerabilities Section.

When all the information is input to the visible screen, you can scroll the screen using the right side vertical scroll bar or use the question selector in the lower left corner to get to the question desired. Note that the selector shows #3 which is the question row selected with a right arrowhead.

As before, when finished:

- Left Click on <Close> button in the lower right corner to go back to the Assessment Screen.

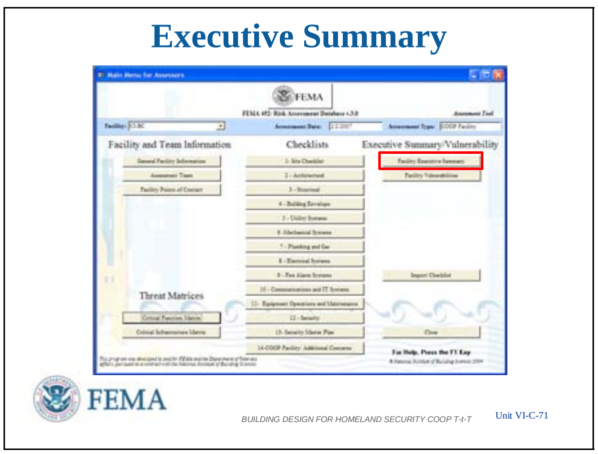
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-70

Assessment Tool – Checklists (6 of 6)

The remaining buttons in the Checklist column all function the same way to capture observations and recommendations or remediations.

VISUAL VI-C-71

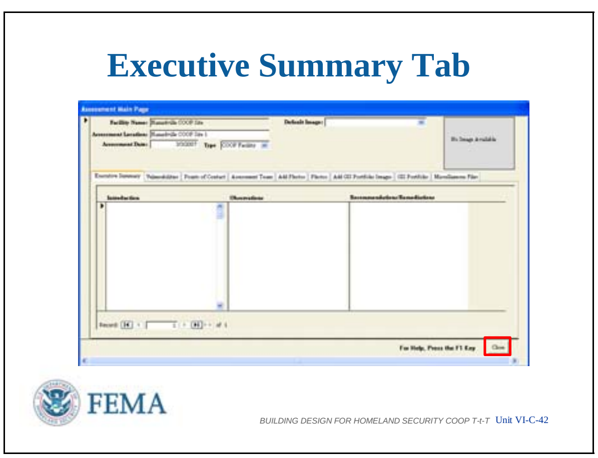


Assessment Tool – Executive Summary (1 of 2)

The Facility Executive Summary section of the Assessment Tool allows an Assessor, usually the Lead Assessor, to write a page to summarize general information about the facility and this assessment.

- Left Click on <Facility Executive Summary> button will take you to that screen.

VISUAL VI-C-72



Assessment Tool – Executive Summary (2 of 2)

The Facility Executive Summary section of the Assessment Tool provides three fields for the Lead Assessor (or Team Leader) to summarize general information about the facility and this assessment. When printed, these three fields appear as a single document with three main sections:

- Introduction
- Observations
- Recommendations / Remediations.

The Introduction field should contain some background information, site location, mission, dates, etc.

The Observations field should contain general information about what was found, but particularly, vulnerabilities. Are they security related, critical infrastructure related, etc?

Finally, the Recommendations / Remediations field is for general recommendations about current conditions, mitigation measures that are applicable to the major vulnerabilities and other pertinent information to consider.

You can use the tabs above the three fields to go from this section to any other in order to review information as necessary while writing the Executive Summary.

One word of caution regarding the Executive Summary: The import/export utility will not transfer this section of the tool between Assessors, so if an assessment team member other than the Lead Assessor fills in these fields, there are two ways to transfer the information between laptops:

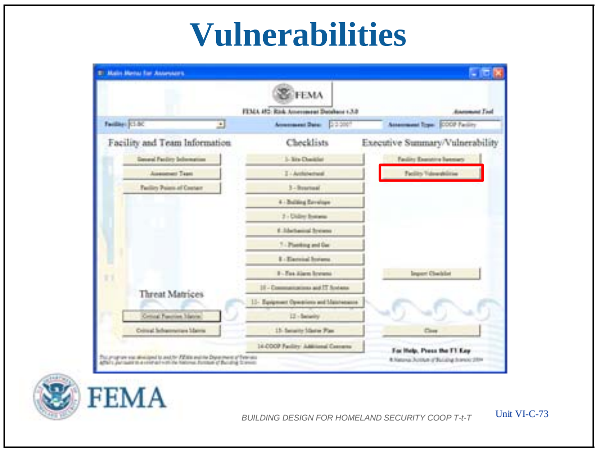
- Method 1: The drafter of the Executive Summary switches to Master Database mode, goes to Site Reports / Executive Summary / Publish as a Word Document / Save the Word Document where it can then be transferred to the Lead Assessor as a Word Document file.
- Method 2: The drafter cuts and pastes the three paragraphs into a document and transfers the temporary document between computers.
- By either method the Lead Assessor can cut and paste the individual paragraphs back into the Executive

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Summary.

- Left Click <Close> to return to the Main Menu for Assessors Screen.

VISUAL VI-C-73

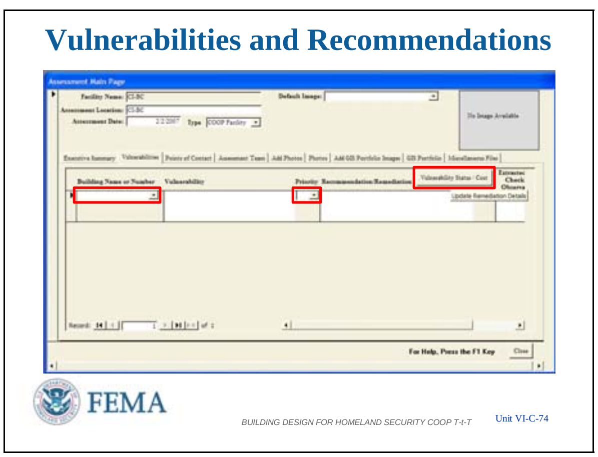


Assessment Tool – Vulnerabilities (1 of 4)

The Facility Vulnerabilities section of the Assessment Tool operating mode provides a means to further analyze the vulnerabilities found during the assessment. By displaying on one list the site's vulnerabilities, their location and the initial recommended remediation, assessors can determine common weaknesses and mediation strategies that will work for multiple vulnerabilities. This also aids in the analysis of prioritization for mediation.

- Left Click on <Facility Vulnerabilities> button will take you to that screen.

VISUAL VI-C-74



Assessment Tool – Vulnerabilities (2 of 4)

This is the Vulnerability and Recommendation screen of the Assessment Tool operating mode.

It is automatically populated with the previously entered Observations and Recommendation / Remediation when the "Vuln?" box is checked upon completing a checklist question. Thus, the assessor believes that there is a sufficient Vulnerability rating to this Observation that remediation action should be identified and tracked.

Note that the rightmost column of the page shows the checklist section from where vulnerabilities were transferred. Assessors can also populate the list by typing vulnerabilities onto the page (for example, a vulnerability identified that may not be associated with a checklist question).

This screen has two fields that must be completed as indicated when the checklist "Vuln? Box was checked:

Left Click to get red box around Building Name or Number Box

- Record a <u>building name or number</u> in the first column to focus where this vulnerability is located.

Left Click to get red box around Priority Box

- <u>Prioritize the vulnerability</u> so as to better identify which vulnerabilities require mitigation based upon the limited resources available – get the best benefit / cost ratio for reducing overall risk.
    - **CAUTION**: If a priority of 1-5 is not entered before the inputs are accepted by the database, the number will be set to zero and this entry will come out on the top of the vulnerability report.
    - Prioritization is based on the severity of the vulnerability and the availability of resources for mitigation as determined by the Program Manager or owning organization. For example: Priority 1 vulnerabilities are the most important to mitigate…fix it now. Priority 5 vulnerabilities can wait until extra funds are available.

The Master Database can be <u>searched based on this field</u>…all Priority 1 vulnerabilities, all Priority 1 and 2 vulnerabilities, etc.

There are two other ways to get Vulnerabilities and Recommendations / Remediations into the fields:

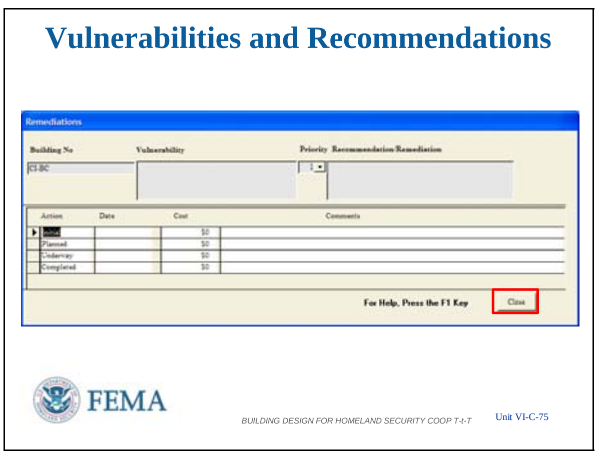
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- The Assessors can <u>type them directly</u> into the fields. They will not show linkage to specific checklist questions unless that information is also added.
- Vulnerabilities and Recommendations / Remediations can be <u>imported</u> from the Assessment Tools of other Assessors using the tool's import utility. In doing this, the Lead Assessor has the option of importing all of a Team Member's vulnerabilities and recommendations, or choosing specific ones to transfer.

Left click to bring up red box around <Vulnerability Status / Cost>

- Left Click on <Vulnerability Status / Cost> from the Vulnerabilities screen to enter the Remediation module.

VISUAL VI-C-75



Assessment Tool – Vulnerabilities (3 of 4)

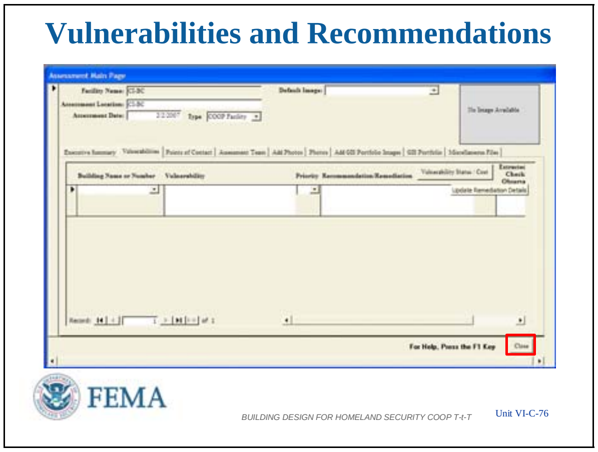
Finally, the Assessment Tool allows an assessment team to provide a cost estimate (dollar values) to the individual recommendations: New fence $100,000, Vehicle barriers $25,000, etc.

- The Program Manager can then track the cost information throughout the process to implement the recommendation.

- Left Click on <Close> to exit the Remediations screen

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

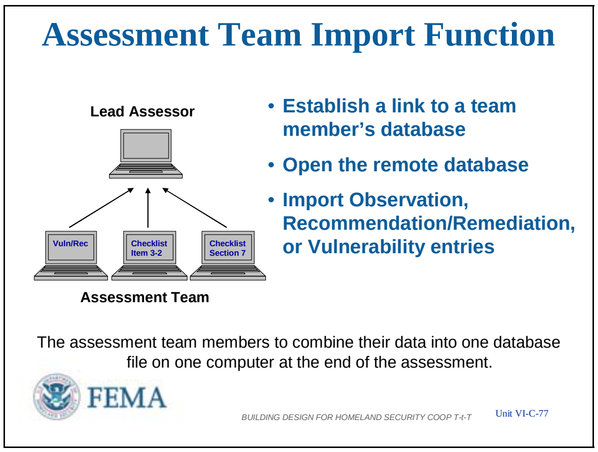
VISUAL VI-C-76



Assessment Tool – Vulnerabilities (4 of 4)

- Left Click on <Close> to exit the Facility Vulnerabilities screen

VISUAL VI-C-77



Assessment Tool – Import Assessment Information – Linking (1 of 8)

NOTE to instructor: Tell students to follow the presentation on the projection screen as the import function requires a separate database with content. Recommend telling students to tilt down the screen on their laptop.

After the assessment team has completed its data collection effort, the checklist questions, vulnerabilities, and remediations have to be combined into one database before the data can be transferred to the Master Database. This is accomplished by using the import function to transfer collected data from the Team Members Databases to the Lead Assessor's Database.

Let's say there are five members of the assessment team: A Lead Assessor, a Security Specialist, a Mechanical/Electrical Assessor, a Structural Engineer, and a Cost Estimator. Before the start of the assessment, the Lead Assessor (or Team Leader) should assign Checklist sections to each member of the team. For example, the Structural Engineer would do Checklist Sections 2, 3

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

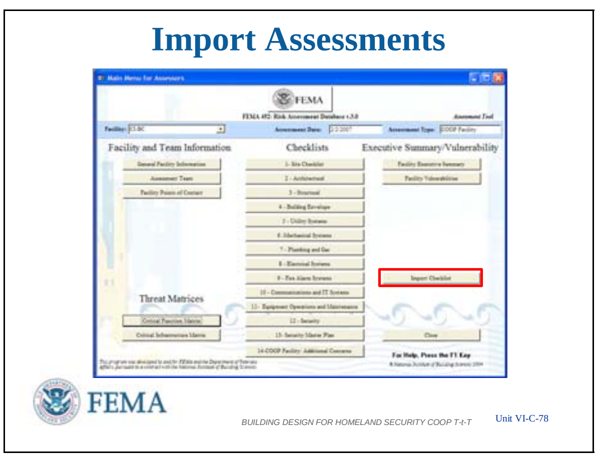
and 4. Checklist sections can be split among team members; this makes importing only slightly more complex.

The import utility of the Assessment Tool allows the Lead Assessor to collect checklist observations and comments, along with vulnerabilities and the associated recommendations from the team members. This consolidated database is the responsibility of the Lead Assessor to ensure technical editing, consistency, and a flowing report to become part of the Master Database.

The process is simple but it takes some practice. The steps to remember are:

- The Lead Assessor must be in the "Admins" user group.
- Establish link to team member's database
- Open the remote database
- Import Observation, Recommendation / Remediation, or Vulnerability entries

VISUAL VI-C-78



Assessment Tool – Import Assessment Information – Linking (2 of 8)

First, ask your database administrator to make sure the Lead Assessor user name is assigned to the "Admins" user group.

Left Click to display red box around <Import Checklist> button

<u>If you are not in the "Admins" user group, the Import Checklist button will be grayed out and not functional.</u>

The next step is to establish a link between the Lead Assessor's database and a copy of the team member's database.

Each team member must copy his Assessment database file to a transfer device -- a USB drive works well. The file will be a

INSTRUCTOR NOTES	CONTENT/ACTIVITY

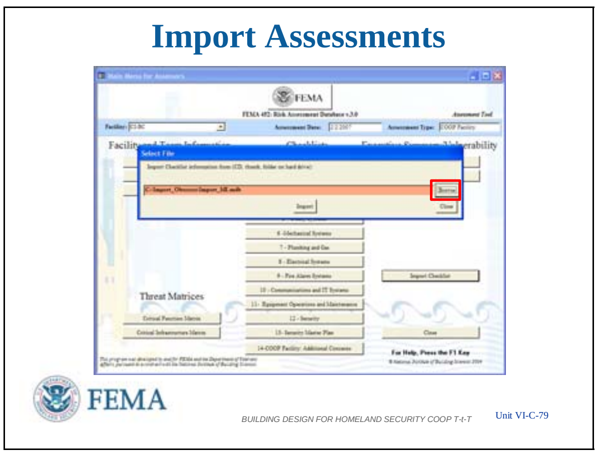
large (several dozen megabyte (MB)) Microsoft Access© .MDE database file. A CD could also be used.

The Lead Assessor inserts the USB drive into his own laptop and copies the file into a working folder for the assessment site with a readily identifiable file name.

Then, from the Main Menus for Assessors, the Lead Assessor should select the facility being assessed from the pull down list.

To begin the Import Function, Left Click on <Import Checklist> button

VISUAL VI-C-79



Assessment Tool – Import Assessment Information – Linking (3 of 8)

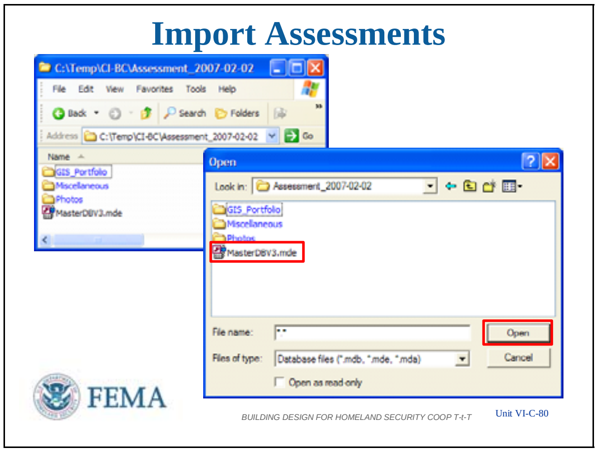
This brings up a request window to identify the file to select for import.

The file entry may default to the FEMA 452 database you installed or the last database that was imported.

Left Click on <Browse> to find the file. This brings up a red box around <Browse>.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-80



Assessment Tool – Import Assessment Information – Linking (4 of 8)

The rear screen is one example of where the assessor file to import can be loaded. In this case, in the root directory C:\ in a Temp (Temporary) folder.

The front screen is what <Browse> takes you to when seeking the needed .MDE file to import. Note the GIS Portfolio, Miscellaneous, and Photos subfolders are also contained in the Temp folder.

NOTE to instructor**:** Just as the GIS Portfolio Images, Miscellaneous Files, and Photos had to be placed into the appropriate subfolders, each Team Member must also provide these files on the USB thumb drive or other media for transfer to the Lead Assessor’s computer and placement in the proper folders.

After finding the .MDE database file either double Left Click on the file

OR

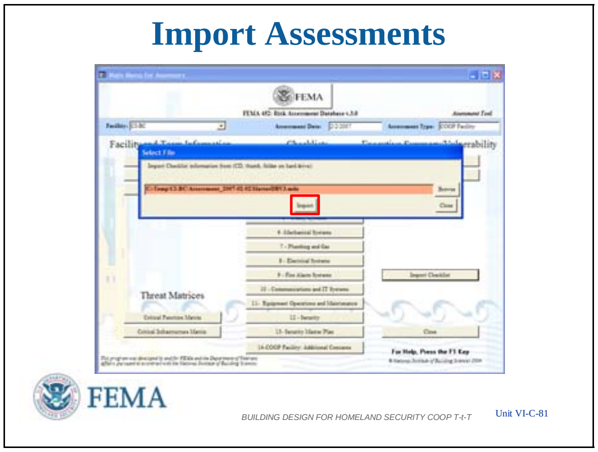
Left Click once on the file to have the file name and location appear in the File Name to Open

AND

Left Click once on <Open> button to link.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-81



Assessment Tool – Import Assessment Information – Linking (5 of 8)

You should now see the path and filename for the .MDE database you want to import.

Finish initiating the process:
Left Click on <Import> button.

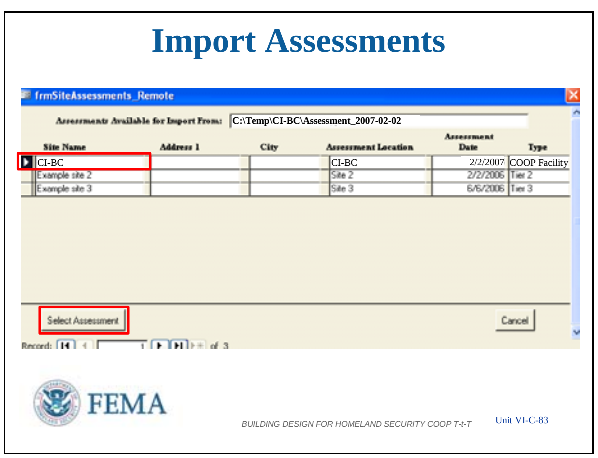
VISUAL VI-C-82

Assessment Tool – Import Assessment Information – Linking (6 of 8)

You then get a confirmation screen

Left Click on <OK> button to continue.

VISUAL VI-C-83



Assessment Tool – Import Assessment Information – Linking (7 of 8)

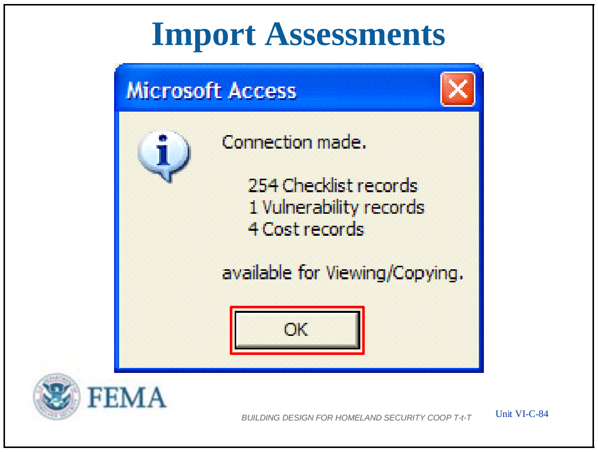
This will bring up a window listing all the available assessment sites available to import.

Left Click on the assessment site you want to link with in the first column. Selection is verified with the right facing arrowhead.

Then click on <Select Assessment> to establish a connection between databases.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-84



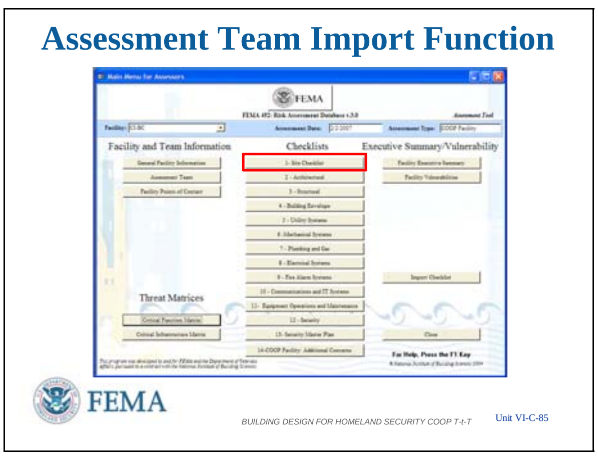
Assessment Tool – Import Assessment Information – Linking (8 of 8)

This brings up a small window to indicate the connection between databases has been made, and # of Checklist records and # of Vulnerability records available for viewing and copying to the Lead Assessor's database.

Warning: It is important to realize that the wrong database can be imported as easily as the correct one. It is imperative for the Lead Assessor to keep accurate track of files copied from other Assessors.

Click on <OK> to continue.

VISUAL VI-C-85



Assessment Tool – Import Assessment Information – Accessing (1 of 3)

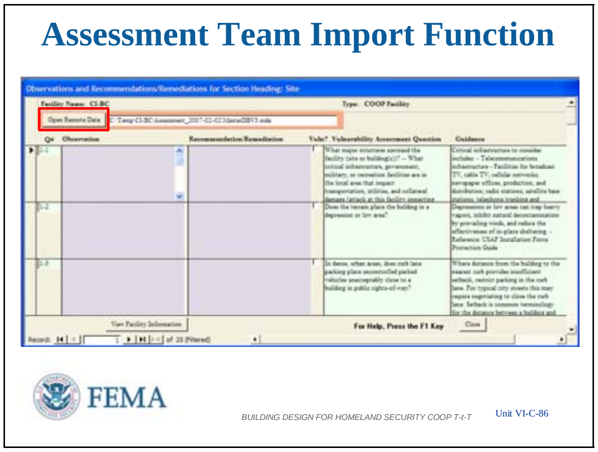
Once the link is complete, then selecting the desired data and bringing it into the Lead Assessor's database is the next step.

The Lead Assessor goes to the Main Menu for Assessors and selects the Checklist Section he wants to import.

We will use the Site Checklist to illustrate: Left Click on <1 – Site Checklist>.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-86

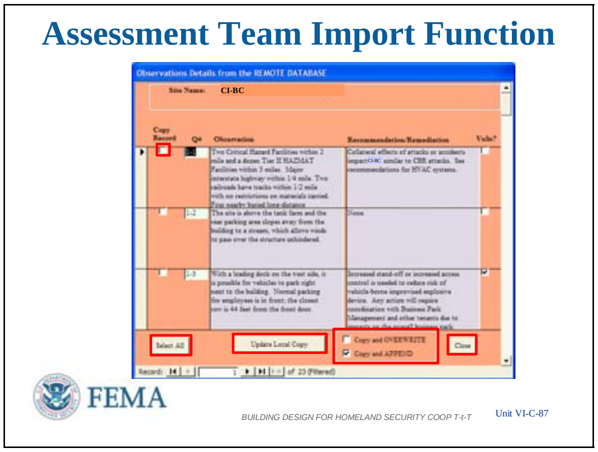


Assessment Tool – Import Assessment Information – Accessing (2 of 3)

The next screen is the standard checklist screen with one addition – there is a tab <Open Remote Database> and a window showing the linked database all framed in orange.

Left Click on <Open Remote Database> tab to begin selecting data for importing.

VISUAL VI-C-87



Assessment Tool – Import Assessment Information – Accessing (3 of 3)

The next screen shows the information in Section 1, Site Checklist, of the Remote Database.

The Lead Assessor can then select the specific observations and comments he wants to import by putting a check mark in <Copy Record>

Left Click will put red box around <Copy Record>

OR

The Lead Assessor can select everything by putting a check mark in <Select All>

Left Click will put red box around <Select All> button

The Lead Assessor has two options for how the new information is entered:

Left Click will put red box around the Copy box

- A checkmark in the <Copy and Append> box will add the information to what is already entered without changing the existing information.
- A checkmark in the <Copy and Overwrite> will overwrite anything

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

previously entered.

- The default is <Copy and Append>.

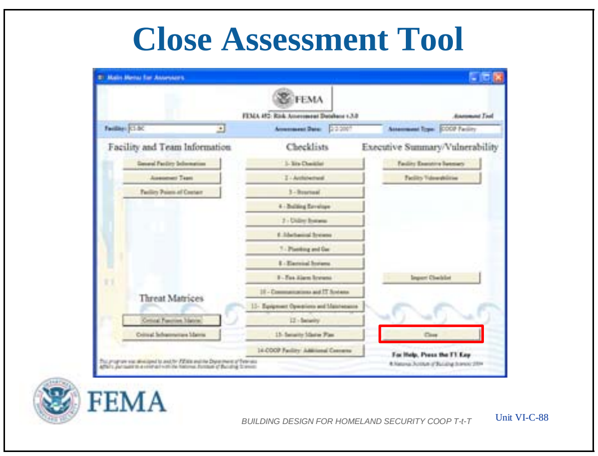
After making some or all selections to transfer to the Lead Assessor database the Lead Assessor must update his copy:
Left Click will put red box around <Update Local Copy> button

The process is the same for importing the other checklists.

This is a very handy tool, allowing the Lead Assessor to have all of the collected data in one computer in one database before leaving the site at the end of the assessment.

Left Click on <Close> button to close the remote data selection window.
This takes you back to the Main Menu for Assessors screen.

VISUAL VI-C-88



Close Assessment Tool

We have seen all the features of the Main Menu for Assessors

Now it is time to return to the Main Menu of the Assessment Tool operating mode.

Left Click on <Close> button.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-89

Empty Assessment Database -- Erasing All Assessments in the Assessment Tool

Left Click to display red box around <Empty the Database> button.

In Version 3.0, the Assessor or Program Manager with a user name in the “Admins” user group have the capability to erase all records in an Assessment database, **permanently**. This is only done after transferring the data to a Master Database and when starting a new assessment. This enables an Assessor to start with an empty database for a new assessment or assessment year. As shown before, preliminary information will have to be loaded into the database prior to performing each assessment or the information will have to be loaded on site.

WARNING: Confirm you have transferred the information to the Master Database before you erase the data.

It is recommended that the old database be stored on a CD for reference during future assessments.

NOTE to instructor: If you did Left Click on <Empty the Database> you will get a screen that will seek confirmation that you want to **permanently** erase all assessment data.

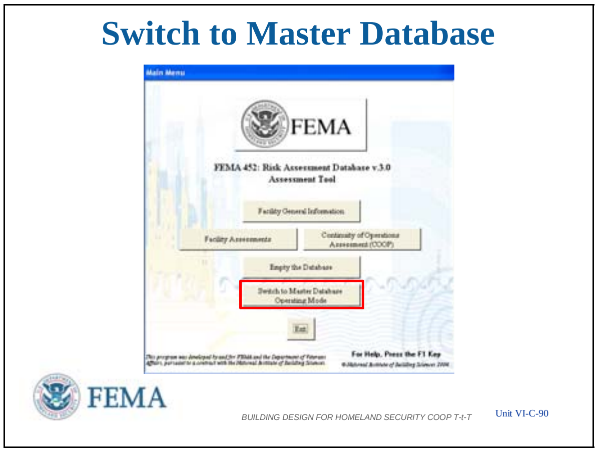
Left Click on <Yes> to continue the emptying of the database

OR

Left Click on <No> or <Cancel> to stop the process and retain all information in the database.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-90



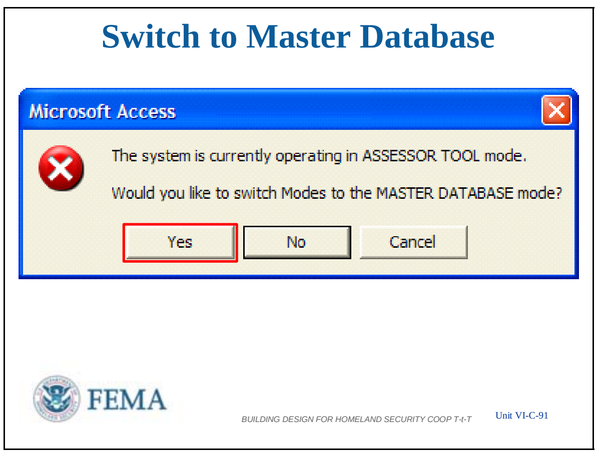
Switch to Master Database Mode (1 of 3)

The last item on the Main Menu of the Assessment Tool is the ability to switch to the Master Database operating mode.

NOTE to instructor: Tell students that they can now follow along with their laptops if they so desire.

Switching is as simple as:
Left Click on <Switch to Master Database Operating Mode> button.

VISUAL VI-C-91

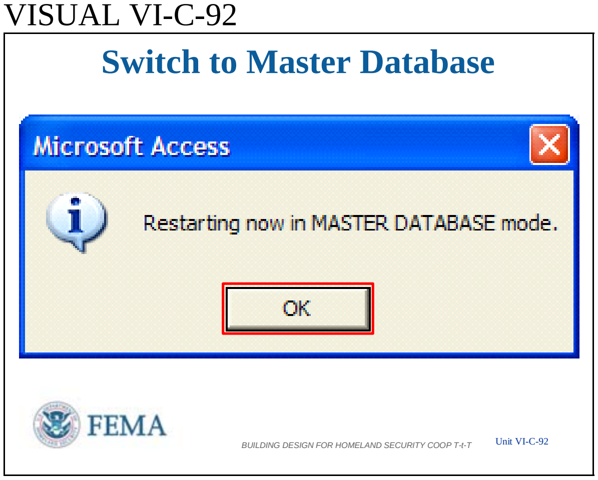


Switch to Master Database Mode (2 of 3)

The next window confirms that you want to switch modes.

Left Click on <Yes> to continue or the other buttons if you do not want to change modes.

VISUAL VI-C-92

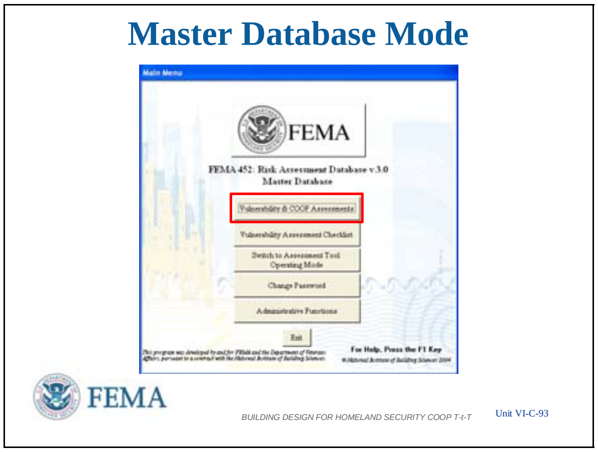


Switch to Master Database Mode (3 of 3)

Then another confirmation window pops up. Left Click on <OK> to complete the switch.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-93



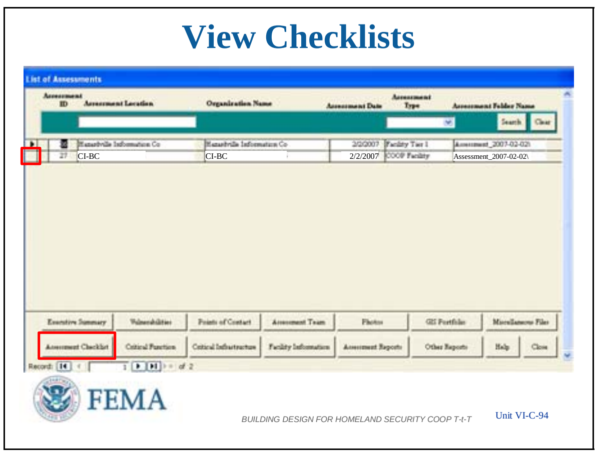
Master Database Mode

The Assessment Function gives the Program Manager or an Assessor the ability to review assessment data, photos and files, search for specific observations, vulnerabilities, etc.

Printing reports from individual sites or from the results of searches is also a Master Database mode capability.

- Left Click on <Vulnerability & COOP Assessments> button.

VISUAL VI-C-94



Master Database – Checklists (1 of 2)

This form provides the Program Manager the ability to review assessment data, photos and files; search for specific observations, vulnerabilities, etc.; and print reports from individual facilities or from the results of the searches.

The first step is to select one of the assessments by Left Clicking on the far left column of the List of Assessments.
Left Click to display red box for selection.

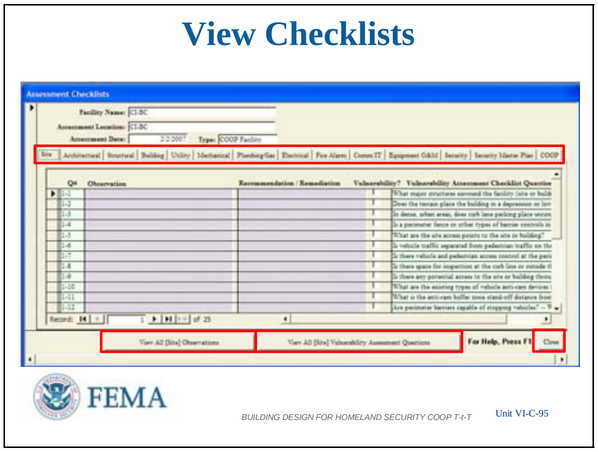
This will mark the assessment desired with a right pointing arrowhead if one is not already there. This indicates selection of the assessment and links the buttons across the bottom to that assessment.

All underlying screens mirror the screens for the same named items in the Assessment Tool operating mode, except for the Assessment Checklist.

- To investigate Left Click on <Assessment Checklist> button.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-95



Master Database – Checklists (2 of 2)

As can be seen the initial screen is a summary type slide showing the Site Checklist questions as that is the initial default tab.

You have access to all the checklists using the tabs above the list.

Left Click to display red box around checklist tabs.

Left Click on any cell of a row selects that row and retrieves underlying screens that look much the same as in the Assessment Tool.
OR
Left Click on <View Site Observations> button provides a screen that looks much like the Assessment Tool data entry screen.

Left Click to display red box around <View Site Observations> button.

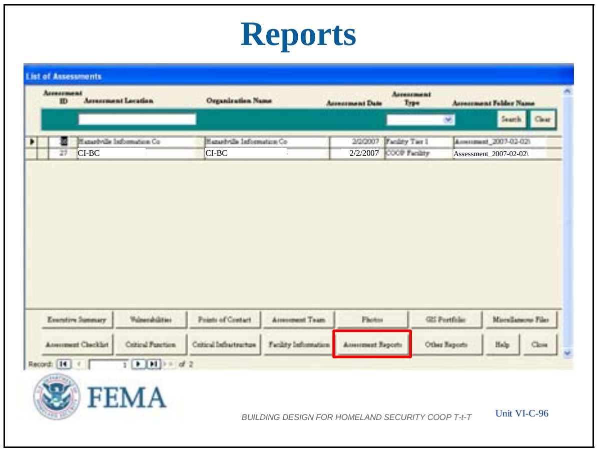
Similarly, Left Click on <View All Site Vulnerability Assessment Questions> will make the Checklist Questions and Guidance more accessible and easier to read.

Left Click to display red box around <View All Site Vulnerability Assessment Questions> button.

- Left Click on <Close> to return to the List of Assessments

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

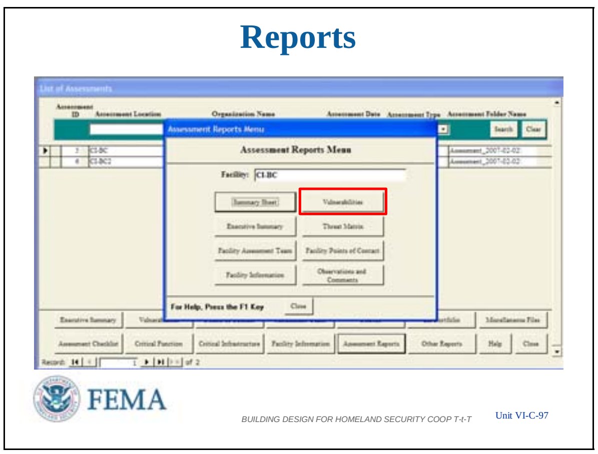
VISUAL VI-C-96



Master Database – Reports (1 of 9)

- Left Click on <Assessment Reports> button to bring up the standard reports.

VISUAL VI-C-97

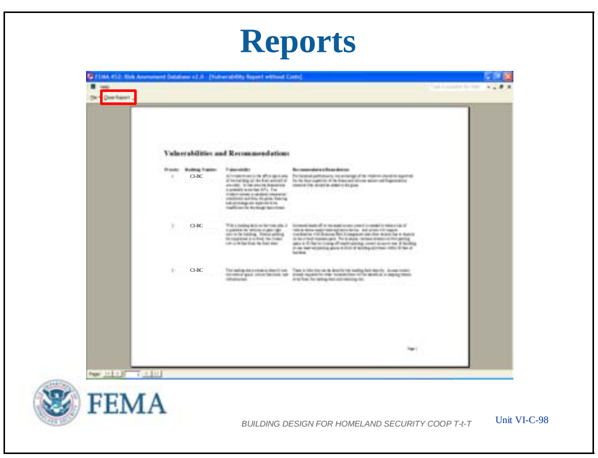


Master Database – Reports (2 of 9)

Here are the standard reports available.

- Left Click on <Vulnerabilities> button to illustrate a report that is expected to get a lot of use.

VISUAL VI-C-98



Master Database – Reports (3 of 9)

The Vulnerabilities and Recommendations report comes out as a Word® Document.

This report can be sent to a printer or published and saved as a Word® Document using the <File> Pull-down Menu in the upper left corner.

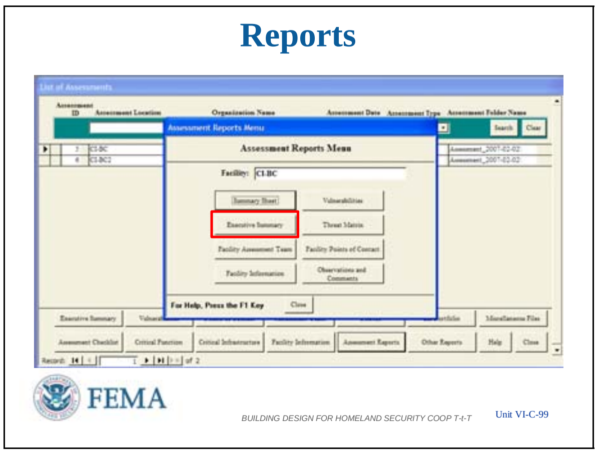
Left Click to display red box around <File>

Caution: If you forgot to prioritize any vulnerability, they will default to “zero” and show up at the top of this report.

To close the report you will also find the <Close Report> button in the upper left corner vice the lower right corner as found on data entry screens.

- Left Click on <Close Report> button

VISUAL VI-C-99



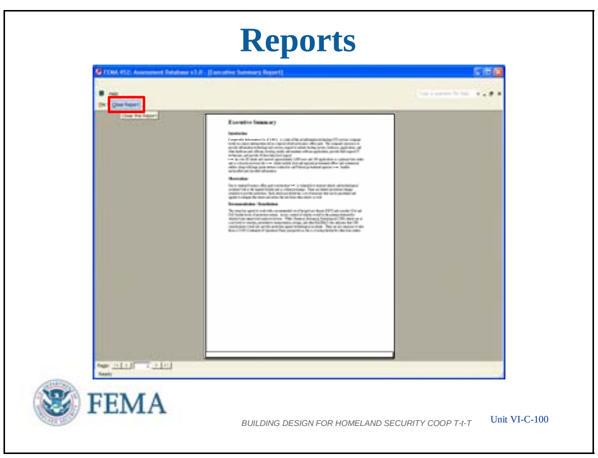
Master Database – Reports (4 of 9)

Similarly, the Executive Summary can be printed directly or published and saved as a Word® Document.

Thus, the intent is to make it very easy to collect information from the Master Database to be able to cut and paste into a Word® Document report or Power Point® Presentation.

- Left Click on <Executive Summary> button

VISUAL VI-C-100



Master Database – Reports (5 of 9)

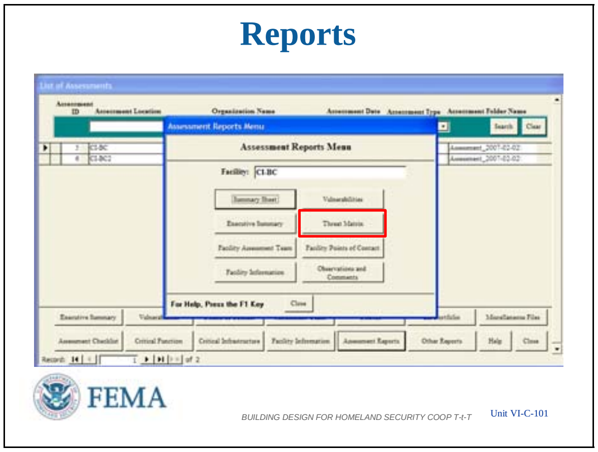
Just like Vulnerabilities, the Executive Summary is a Word® Document with the same ability to print, publish, or save to include in other documents.

Since you have not inputted any Executive Summary information, your screen will only show the headings.

- Left Click on <Close Report> button

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-101

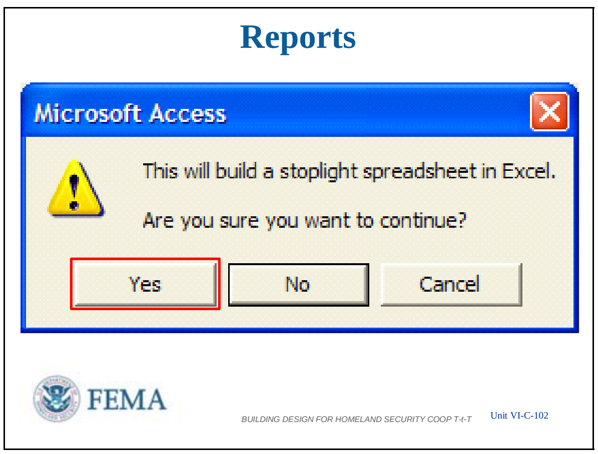


Master Database – Threat Matrix (6 of 9)

Re-entering the Assessment Reports Menu, continue the review by looking at the Threat Matrix.

- Left Click on <Threat Matrix> button

VISUAL VI-C-102

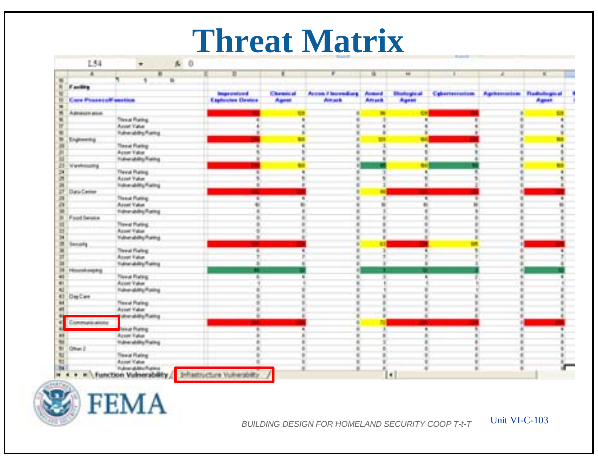


Master Database – Threat Matrix (7 of 9)

This Report gets generated as an Excel® Spreadsheet as seen in the confirmation pop-up.

- Left Click on <Yes> button to continue.

VISUAL VI-C-103



Master Database – Threat Matrix (8 of 9)

The spreadsheets build in sequence starting with Critical Functions, then Critical Infrastructure.

- Left Click on <Critical Functions> tab.

Since a user can not change the headings in the database in Version 3.0, here is one way to ensure the threats, functions, and infrastructure headings are tracked by the general user.

- For example, The Core Process / Function labeled in the database as Other 1 can be

INSTRUCTOR NOTES	CONTENT/ACTIVITY

changed to Communications.

Left Click to advance slide and show the change.

NOTE to instructor: In Version 4.0, the Program Manager will be able to change:

- Threats
- Hazards
- Critical Functions
- Critical Infrastructure.

Also you need not enter information in all rows and columns if the Function or Threat is not applicable to that assessment.

- See Food Service in the Function column and Arson / Incendiary Attack in the Threat row, respectively.

The spreadsheet is Fully Interactive – any rating cell can be changed resulting in new totals and color adjustments in accordance with the risk assessment scale. Changes to any cell can be printed or saved with these changes.

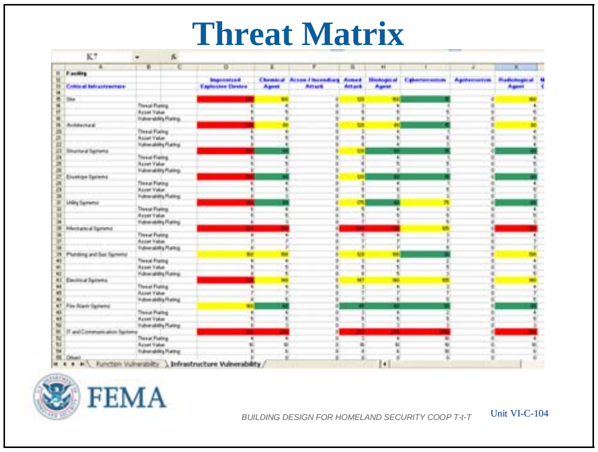
- **Caution**: Changes made to either Spreadsheet do not work back into the Master Database. Those changes would have to be input separately into the database.

- Left Click on <Critical Infrastructure> tab to see that spreadsheet.

NOTE to instructor: When the spreadsheet completes building, the Critical Infrastructure is displayed. The reason to go to Critical Functions first was to familiarize the students with this spreadsheet feature.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-104

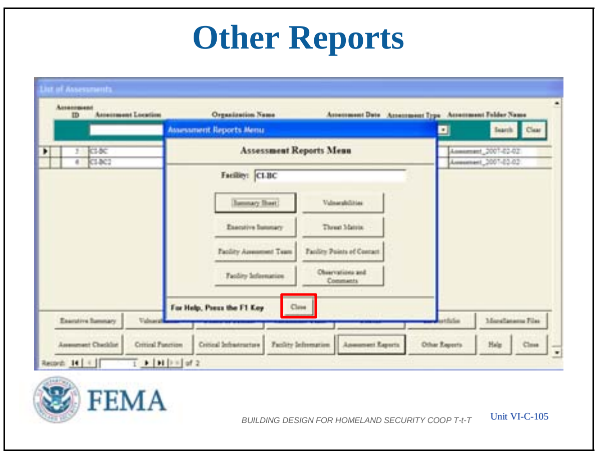


Master Database – Threat Matrix (9 of 9)

The Infrastructure Threat Matrix spreadsheet has all the same features as the Function spreadsheet just illustrated.

- Left Click on <Red X Box> in upper right corner to close out of the spreadsheet.

VISUAL VI-C-105

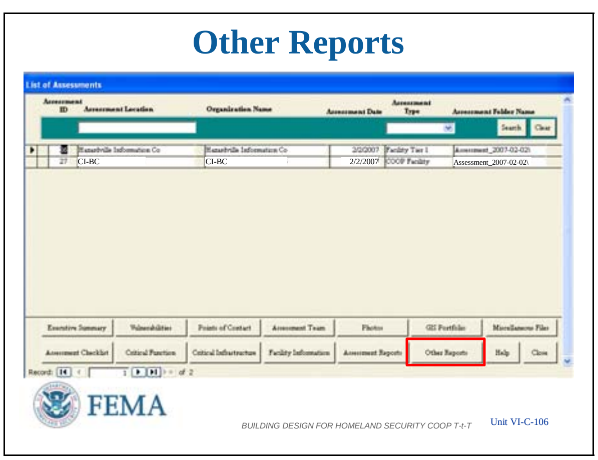


Master Database – Other Reports / Search (1 of 6)

Returning to the Assessment Reports screen we want to review the Other Reports on the List of Assessments screen.

- Left Click on <Close> button just below center of the screen

VISUAL VI-C-106



Master Database – Other Reports / Search (2 of 6)

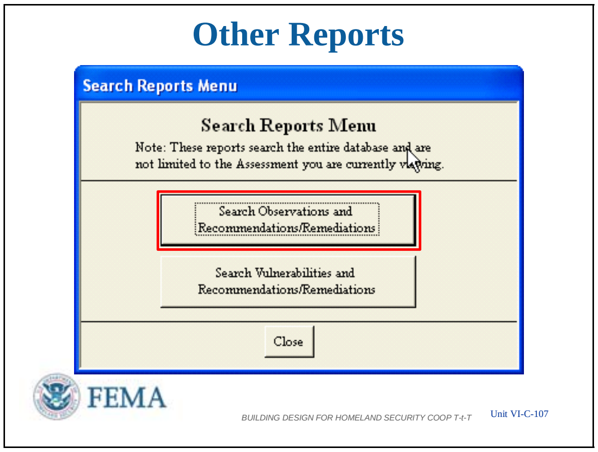
Now from the List of Assessments screen:

- Left Click on <Other Reports> button

This takes us to the Search Function of the Master Database operating mode.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-107



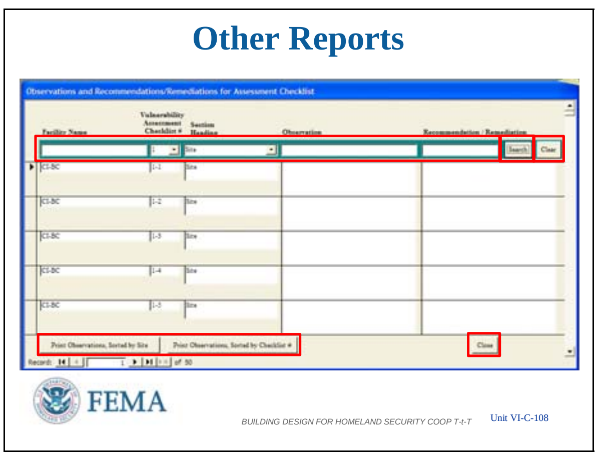
Master Database – Other Reports / Search (3 of 6)

The pop-up screen allows us to search:

- Observations and Recommendations/ Remediations
- Vulnerabilities and Recommendations/ Remediations.

- Left Click on <Search Observations and Recommendations/ Remediations>

VISUAL VI-C-108



Master Database – Other Reports / Search (4 of 6)

The data entry boxes across the top allow selection of any of these inputs or searching on a word or phrase in those boxes throughout the Master Database using the <Search> button at the end of the row.

- Note that to start a new search you should Left Click on <Clear> button next to the Search button, unless you desire to limit the search based upon the previous search performed.

Printing the Searches is possible using the buttons in the lower left:

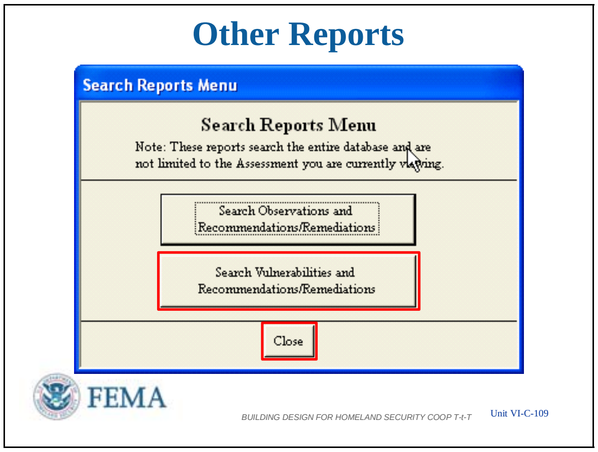
Left Click to display a red box around these buttons:

- Print Observations, Sorted by Site
- Print Observations, Sorted by Checklist #
  Caution: Limit the number of records to print to 1,000 or less as a pop-up window will appear if this number is exceeded.

- Left Click <Close> to return to the previous screen.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-109



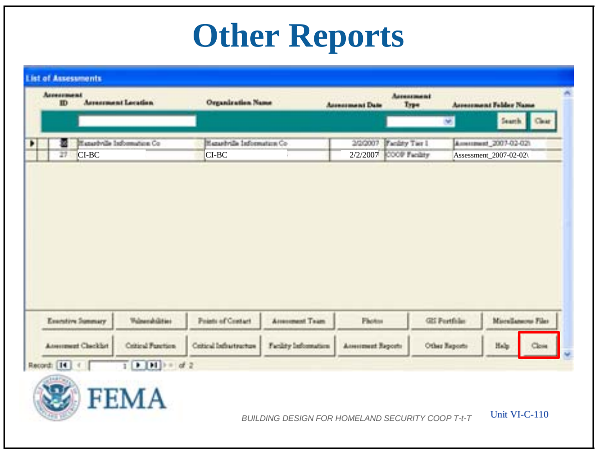
Master Database – Other Reports / Search (5 of 6)

Likewise the other selection on the Search Reports Menu will allow you to Search Vulnerabilities and Recommendations / Remediations. This is a more focused search of this subset of the overall Observations and Recommendations.

Left Click to display red box around <Search Vulnerabilities and Recommendations / Remediations> button

- Left Click on <Close> button in the lower center screen will return you to Other Reports on the List of Assessments screen.

VISUAL VI-C-110

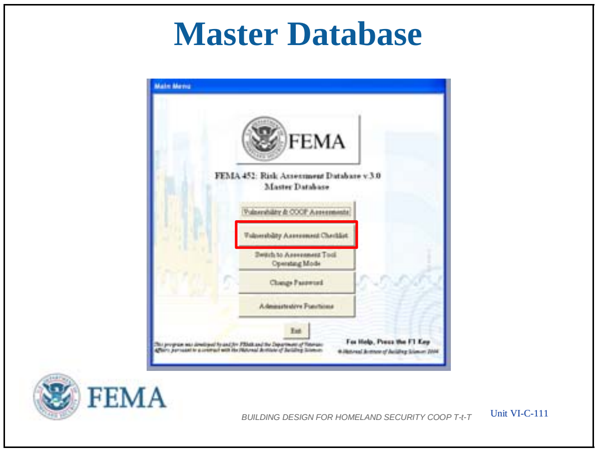


Master Database – Other Reports / Search (6 of 6)

- Left Click on <Close> button in the lower right corner will return you to the Master Database operating mode – Main Menu screen.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-111

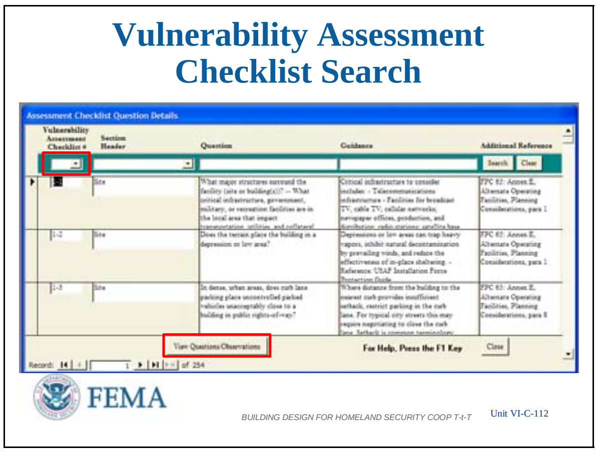


Master Database -- Vulnerability Assessment Checklist (1 of 6)

The Vulnerability Assessment Checklist button gives the Program Manager or Assessor the ability to view all answers for individual checklist questions.
OR
To search for specific content in questions and/or guidance within a section.

- Left Click on <Vulnerability Assessment Checklist> button from the Main Menu.

VISUAL VI-C-112



Master Database -- Vulnerability Assessment Checklist (2 of 6)

This screen shows all observations and recommendation / remediation answers for each assessment checklist question in the database by Section.

Left Click to display red box around Vulnerability Assessment Checklist #

- The drop down menu in the first window of the green search query bar allows the user quick access to the Checklist section.

The right facing black arrowhead indicates the Checklist Question that is selected.

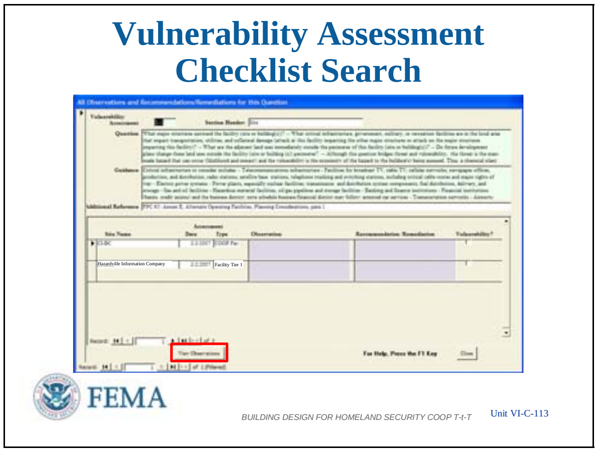
- The <View Questions / Observations> button opens the screen showing All Observations and Recommendations / Remediations in the database for the question selected, Vulnerability Assessment Checklist Question 1-1 in this case.
  - o The question that is displayed is determined by the location of the arrow in the left column, not by the results of any search that was conducted.
  - o The next screen will show this

INSTRUCTOR NOTES	CONTENT/ACTIVITY

question in all the assessments contained in the database.

- Left Click on <View Questions / Observations> to see the selected Question information

VISUAL VI-C-113



Master Database -- Vulnerability Assessment Checklist (3 of 6)

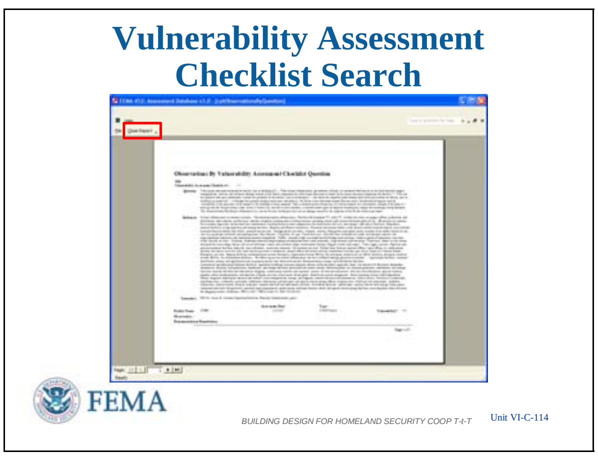
The Checklist Question indicated in the upper left corner has the Question and Guidance at the top for reference.

Then each assessment is listed with the Observation and Recommendations / Remediations so that all Question 1-1 responses (in this case) can be easily reviewed.

The <View Observations> button creates a report of all entries in the database for the designated question, including the question and guidance.

- Left Click on <View Observations>

VISUAL VI-C-114



Master Database -- Vulnerability Assessment Checklist (4 of 6)

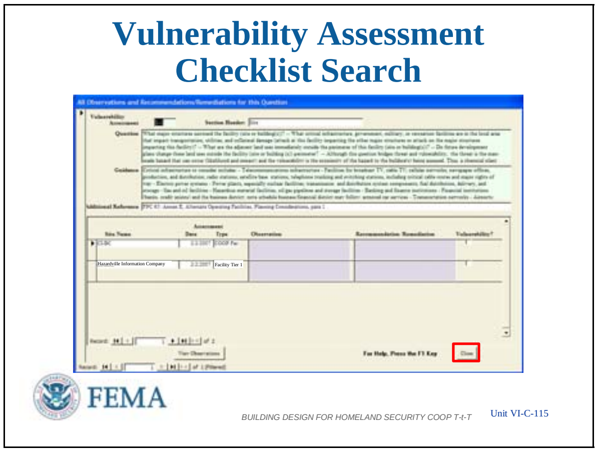
As with the other reports you have seen, this report can be printed or converted to Microsoft Word® for additional editing, formatting, etc.

To return to the "All Observations and Recommendations / Remediations for this Question" screen:

- Left Click on <Close Report> button in the upper left corner

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-115

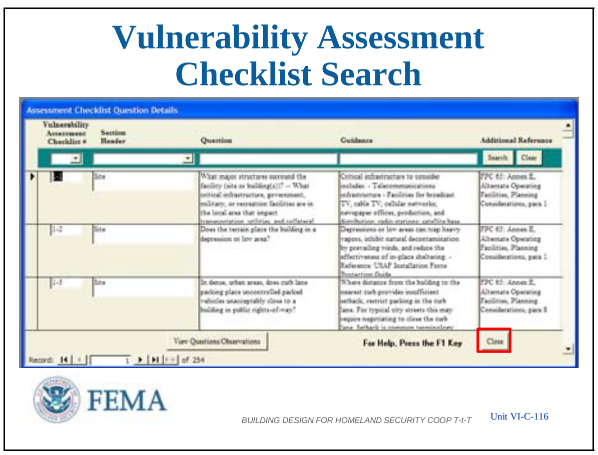


Master Database -- Vulnerability Assessment Checklist (5 of 6)

To go back to the Assessment Checklist Questions Details screen:

- Left Click on <Close> button in the lower right corner

VISUAL VI-C-116



Master Database -- Vulnerability Assessment Checklist (6 of 6)

Left Click to display red box around Question and Guidance in the Search Query window

Keyword searching is also possible, similar to the search routine in the Master Database previously shown.

Left Click to display red box around <Search> button in the Search Query window.

The <Search> button performs search based on criteria entered into the Question and / or Guidance field.

Caution: As before, subsequent searches will only be of the previous results unless the <Clear> button is first Left Clicked.

NOTE to instructor: For searches, the same selection process of the right arrowhead in the left column showing selection still holds. The <View Questions/Observations> button will also provide the same screens as before, but for the questions found in the search.

Left Click to display red box around <Clear> button in the Search Query

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

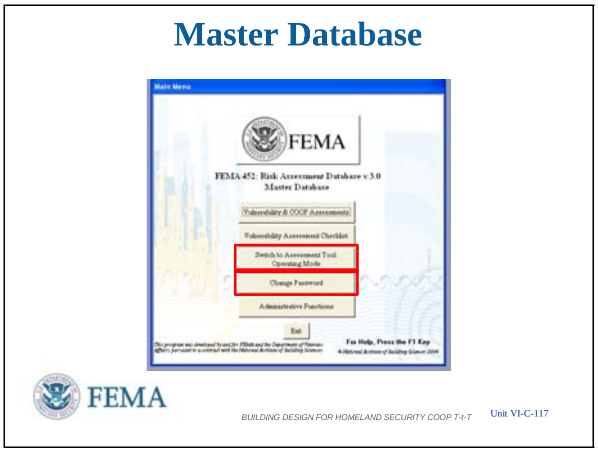
window.

The <Clear> button will allow all questions to be seen again.

To go back to the Master Database Main Menu:

- Left Click <Close> button in the lower right corner

VISUAL VI-C-117



Switch to Assessment Tool Operating Mode and Change Password

MODE

The next item on the Main Menu of the Master Database operating mode is the ability to switch to the Assessment Tool operating mode.

Left Click to display red box around <Switch to Assessment Tool Operating Mode> button in the Search Query window.

Switching is as simple as Left Clicking on <Switch to Assessment Tool Operating Mode> button and then confirming you want to switch modes.

This is the same process as switching from the Assessment Tool operating mode to the Master Database operating mode.

PASSWORD

Each user has the ability to change their password from the Master Database operating mode main menu. When a user is initially created by an administrator (someone with Admins privileges), their password is blank.

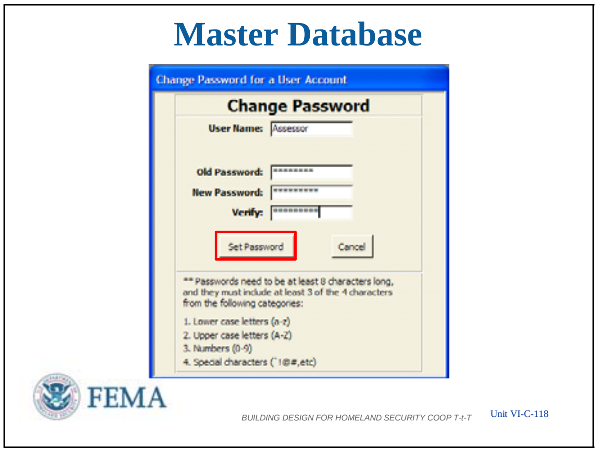
<u>To enter the database the first time, simply enter your user name, leave the password field blank, and Left Click <OK></u>.

It is highly recommended to change your password at your initial entry into the database.

Selecting the <Change Password> button opens the Change Password Form

- Left Click on <Change Password> to see this feature.

VISUAL VI-C-118



Change Password

- Your User name is pre-populated in the top box.
- Enter your existing password in the “Old Password:” box.
- Enter a new password in the “New Password:” box.
- Verify your entry by re-typing the new password in the “Verify:” box.

As shown on this screen, note the restrictions for passwords

- Password must be eight characters long
- Password must include at lease three of the four characters from the following categories:

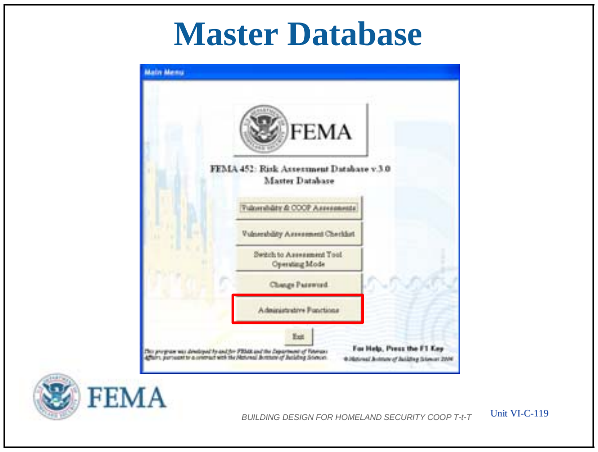
  1. Lower case letters (a to z)
  2. Upper case letters (A to Z)
  3. Numbers (0 to 9)
  4. Special characters (`!@#, etc.)

Left Click <Set Password> to complete the password change.

- Left Click on <Cancel> button to return to Main Menu

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-119



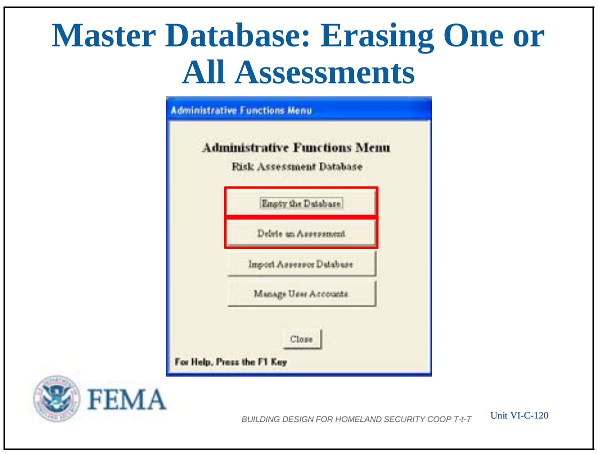
Master Database – Administrative Functions

The final features needed to understand about the Master Database are the most important – the administrative functions. These include:

- Emptying the Master Database (if there is ever a reason to do this)
- Deleting an assessment from the Master Database (more likely if the wrong database is imported)
- Importing the Lead Assessor's Assessment Tool database into the Master Database (expect this to have good use).
- Managing User Accounts

- Left Click on <Administrative Functions> button.

VISUAL VI-C-120



Master Database – Administrative Functions – Erasing Assessments (1 of 2)

Administrators have the ability to erase one or all records in the database, **permanently**.

Empting the Database is usually only done when starting a new program with no past assessments, when starting with a new assessment on a laptop and the database is excessively large, or after archiving past assessments (usually by fiscal or calendar year, but can also be done by facility.

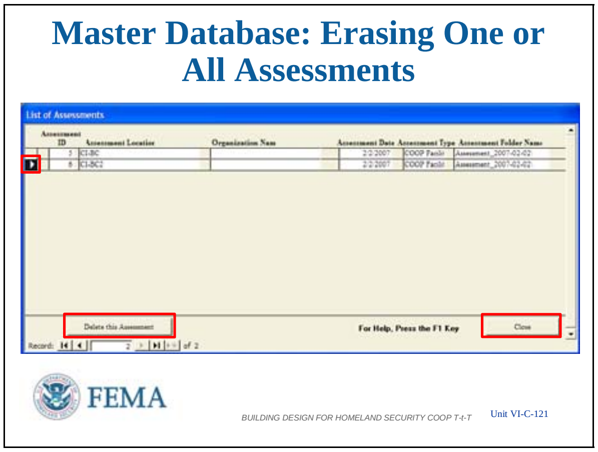
Left Click to display red box around <Empty the Database> button in the Administrative Functions screen.

Selecting the <Empty the Database> button opens a confirmation window, to ensure you want to permanently erase all assessment data. Left Click on <Yes> to continue or <No or Cancel> if you do not.

- Left Click on <Delete an Assessment> button to view this feature.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-121



Master Database – Administrative Functions – Erasing Assessments (2 of 2)

Erasing a Single Assessment in the Master Database is usually only done when an assessment was loaded in error.

Selecting the <Delete an Assessment> button opens a list of assessments as shown in this screen.

Select the assessment to erase by left clicking in any box in that row to turn on a right facing arrowhead at the start of the row.

Left Click on <Delete this Assessment> button. This will open a confirmation window, to ensure you want to permanently erase the selected assessment. Left Click on <Yes> to continue or <No or Cancel> if you do not.

- Left Click on <Close> to return to the Administrative Functions screen.

VISUAL VI-C-122

Master Database -- Import Assessor Database (1 of 12)

Since you do not have a database to import, please tilt down your laptop screens and follow the import procedure with me on the projection screen.

To import an Assessment Database, Left Click on <Import Assessor Database> button.

NOTE to instructor: The import function in Version 2.0 and 3.0 is a one-button operation with some additional linkages later. In Version 1.0, it is a manual operation taking 20 minutes by an Information Technology specialist, such as a Database Manager, knowledgeable in Microsoft Access®.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-123

Master Database -- Import Assessor Database (2 of 12)

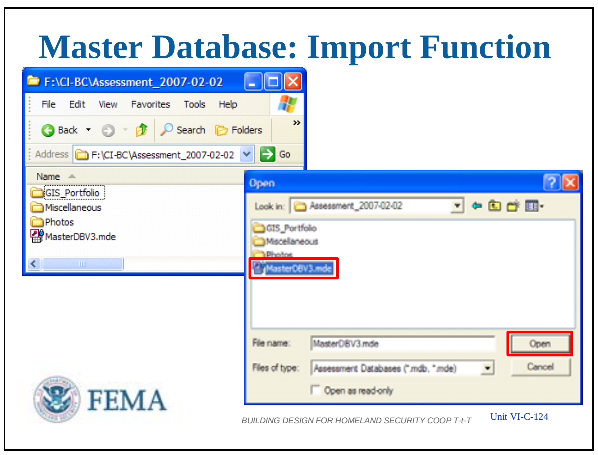
The first step is to find the Assessor database to import.

This screen opens with the file identified to which the Master Database is currently linked.

The process is similar to what the Lead Assessor must do to build the final assessment database with one huge exception.

Left Click on <Find a different Database> button to find the Assessor database that you want to import.

VISUAL VI-C-124



Master Database -- Import Assessor Database (3 of 12)

The rear screen is one example of where the assessor file to import can be loaded. In this case, on a USB thumb drive.

The front screen is what < Find a different Database > takes you to when seeking the needed .MDE file to import. Note the GIS Portfolio, Miscellaneous, and Photos subfolders are also contained on the thumb drive.

NOTE to instructor**:** Just as the GIS Portfolio Images, Miscellaneous Files, and Photos had to be placed into the appropriate subfolders, the Lead Assessor must also provide these files on the USB thumb drive or other media for transfer to the Master Database on the Program Manager's computer.

After finding the .MDE database file either

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

double Left Click on the file

OR

Left Click once on the file to have the file name and location appear in the File Name to Open

AND

Left Click once on <Open> button to link.

NOTE to instructor: While one way of providing pre-assessment information to the assessor laptops is to create an .MDE file with the information already loaded and the subfolders containing available files, the Master Database Import Function can also be used to do the same: Program Manager > Lead Assessors > Assessors using this feature.

VISUAL VI-C-125

Master Database -- Import Assessor Database (4 of 12)

Returning to the Import Assessments screen the Link and Import From window now correctly identifies the database to be imported.

Left Click on <Import> button to initiate the import.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

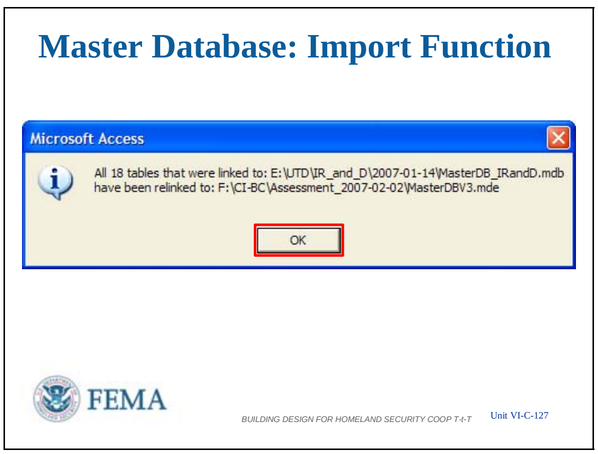
VISUAL VI-C-126

Master Database -- Import Assessor Database (5 of 12)

A confirmation screen then pops up to ensure this is the desired action for the indicated file.

Left Click on <Yes> to continue.

VISUAL VI-C-127

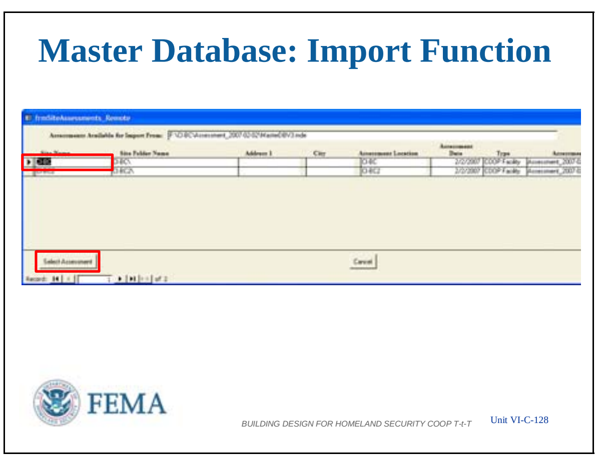


Master Database -- Import Assessor Database (6 of 12)

The import function confirms the linking to the desired database has been accomplished.

Left Click on <OK> button to continue.

VISUAL VI-C-128



Master Database -- Import Assessor Database (7 of 12)

The database may contain more than one assessment. Thus the assessment to import must be selected.

As in other procedures shown before, Left Click on any box in the row to generate a rightward facing arrowhead that designates that this assessment has been selected.

Left Click on <Select Assessment> button to continue importing.

VISUAL VI-C-129

Master Database -- Import Assessor Database (8 of 12)

This is one <u>feature not in the Import Checklist function in the Assessment Tool operating mode.</u>

Instead of manually moving the files in these subfolders between locations as in the Import Checklist function, the Import Assessor Database function of the Master Database allows a one-button operation to do the same thing.

- As with the manual transfers in the Assessment Tool, it is equally important to ensure the file folders in the Remote Database are properly named with the Assessment Location and Date to effect this transfer
  And
- The same file folder names as the Master Database

Left Click on <Yes> to make these transfers.

VISUAL VI-C-130

Master Database -- Import Assessor Database (9 of 12)

The final confirmation pop-up wants to know if you want to write the files now.

Left Click on <Yes> to continue the import process.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

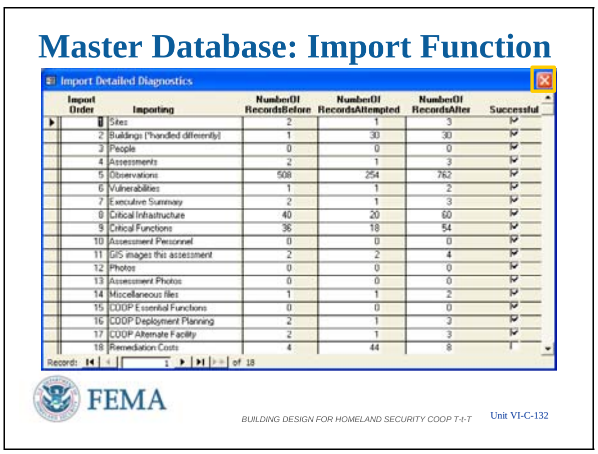
VISUAL VI-C-131

Master Database -- Import Assessor Database (10 of 12)

As in every process, it is always necessary to confirm that what you wanted to have done was actually done.

Next Left Click on <Show Detailed Results> to check that all transfers were successful.

VISUAL VI-C-132



Master Database -- Import Assessor Database (11 of 12)

The Import Detailed Diagnostics screen shows what was in the Master Database before the import, the number of records attempted by the import, and the records after the import.

The quick check is to scan the right hand Successful column to ensure all boxes are checked.

Another check is to scan Row 4, Assessments. The number of assessments being imported should match the number of assessments attempted.

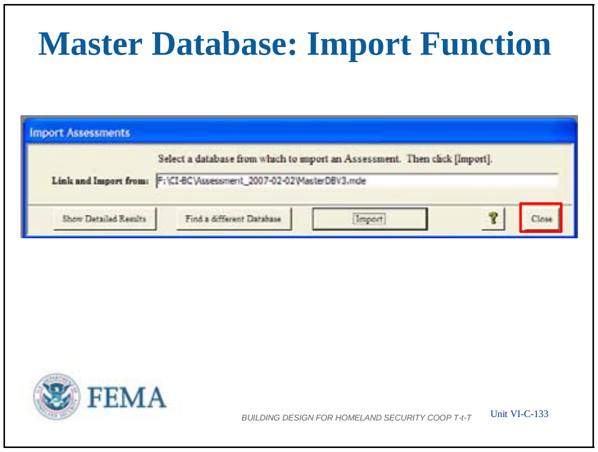
Note that Remediation Costs at the bottom of the list indicates that the transfer was not successful. Two ways to overcome this:

- Delete and start again (probably more desirable)
- Copy the missing information by hand (probably less desirable.

To return to the Import Assessments pop-up, Left Click on <Red X - Box> in the upper right corner to close the window.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-133

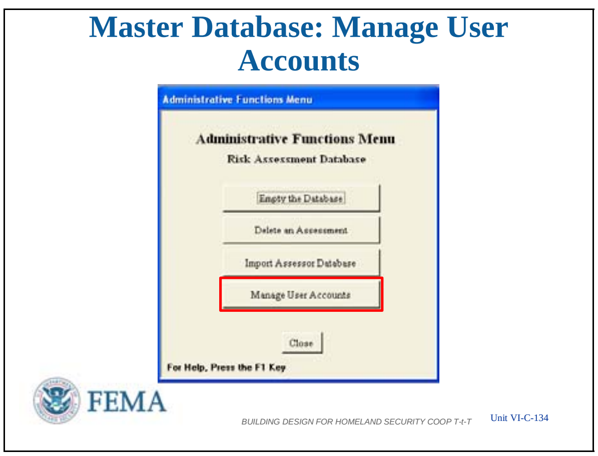


Master Database -- Import Assessor Database (12 of 12)

That completes the import function.

Left Click on <Close> button in the lower right corner to return to the Administrative Functions Menu

VISUAL VI-C-134



Master Database – Manage User Accounts (1 of 4)

You may follow along with your laptops in this final feature.

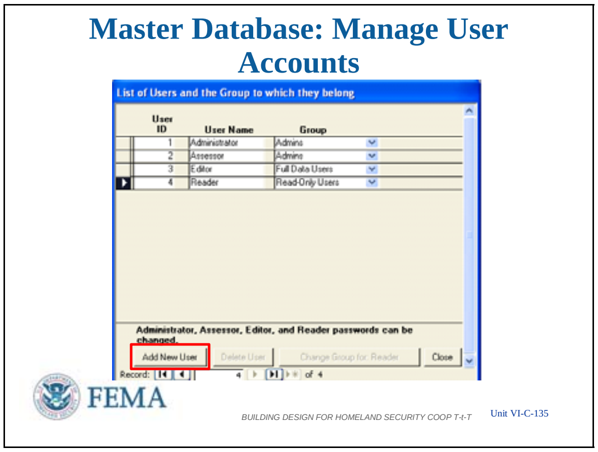
Administrators can manage user accounts using <Manage User Accounts> in the Administrative Functions Menu.

This enables an administrator to add a new user, delete a user, and assign permission levels to users.

- Select <Mange User Accounts> to start the process

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-135



Master Database – Manage User Accounts (2 of 4)

The form labeled “List of Users and the Group to which they belong” is displayed next.

From this form, an Administrator can add a new user, delete a user and assign or change their permission level (called User Group).

User Groups:
Three user groups have been created for the database in the Workgroup File: *Admins*, *Full Data Users*, and *Read Only Users*.

Admins has full access to the database. The Administrative Functions button will only be visible for users in the Administrator group. It is highly recommended to assign the user names “Administrator” and “Assessor” a different password in the Master Database after initial logon.

Full Data Users can view and update data.

Reader can only view data.

- Left Click on <Add New User>

VISUAL VI-C-136

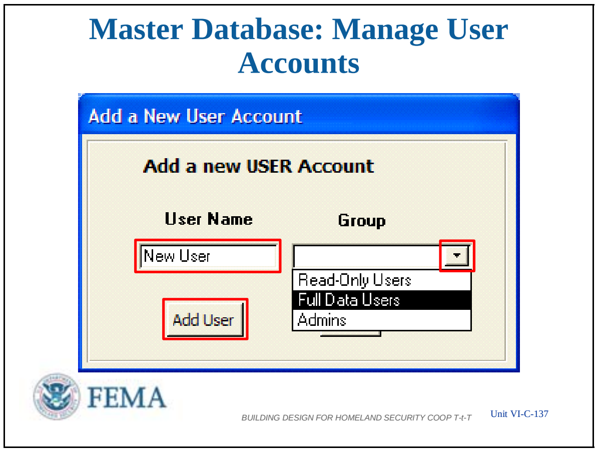
Master Database – Manage User Accounts (3a of 4)

Add a New User Account:
Left Click to display red box around the two windows.
A screen opens called “Add a new USER Account.”

- Type in the new user name
- Select from the drop down box a users group (permission level).

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VI-C-137



Master Database – Manage User Accounts (3b of 4)

Left Click displays a red box around User Name window.

Add a User Name.

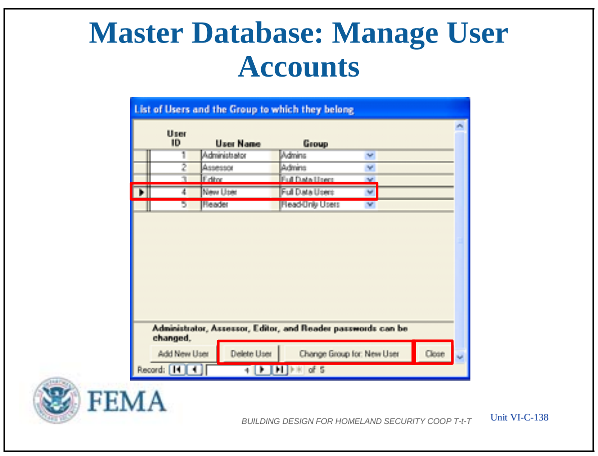
Left Click displays a red box around Group drop down arrow.

Select a Group (permission level) from the drop down menu.

After making entries

Left Click on <Add User> button to finalize the account.

VISUAL VI-C-138



Master Database – Manage User Accounts (4 of 4)

Left Click displays red box around the New User entry into accounts

Left Click displays red box around <Delete User> and <Change Group for > buttons.

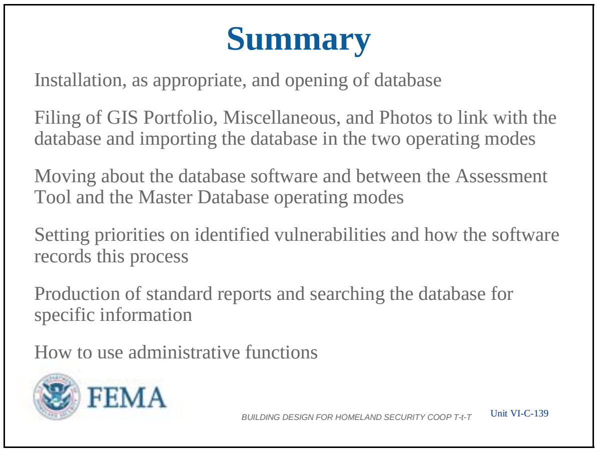
Note that when a new user is added, the <Delete User> and <Change Group for … > buttons become active.

Caution: The four original user accounts can not be deleted. However, the password and permission level for the four original user accounts can be changed.

- Left Click on <Close> button to complete the database presentation.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VI-C-139



Summary

You have been show how to:

- Install, as appropriate, and open the database
- Link collected data to the database and import the database in the two operating modes
- Move around the software and between the Assessment Tool operating mode and Master Database operating mode.
- Handle vulnerabilities, including setting of priorities
- Produce standard reports and searches for specific information showing the benefits of the FEMA 452 databases in performing a Risk Management Program.
- How to use administrative functions – deleting assessments, changing passwords, and managing user accounts.

NO VISUAL

Student Activity

Option 1: The student activity was having the students load the software on their laptops before arriving at the course with the help of their System Administrators. The students then follow along in a Demonstration / Performance instruction methodology.

Option 2: The student activity was having the students with laptops load the software and follow along in a Demonstration / Performance instruction methodology.

Option 3: The student activity will be loading the software on laptops for all those interested at lunch today and/or the end of today. The students will follow the presentation in a lecture mode as there will be no Demonstration / Performance in this option.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	Transition In the next unit, we will investigate the basics of Explosive Blast to better understand the value of mitigation measures presented.

This page left intentionally blank

UNIT VI (C) CASE STUDY ACTIVITY:
FEMA 452 RISK ASSESSMENT DATABASE
(COOP Version)

To this point the assessment procedures have been done manually to understand the thought process. Once the process is understood, the need to be able to manage assessment information, especially from multiple assessments, becomes evident. This unit shows the features of the FEMA 452 Risk Assessment Database v3.0, 16 January 2007, in a demonstration/performance instruction approach or a presentation approach with software installation being done either before arriving at the course or sometime later on Day 2.

Requirements

<u>Minimum hardware and software requirements</u>:

Pentium® 4 or equivalent
Windows XP
MS Access® 2002
256 MB of RAM recommended for all components

<u>Option 1:</u>
Students should have individual personal laptops that they have brought to the course. They have downloaded the database software either from the FEMA Risk Management Series web site or from a FEMA Floodmaps e-mail. They will work with their Systems Administrator as required to ensure the laptop meets the minimum hardware and software requirements listed above and that the software installation is successful. They students may begin familiarization with the software, but that will require some review of the User's Guide.

During the course, the instructor will use PowerPoint slides with database screen captures to illustrate the various features of the software. The database installation slides will be hidden as the laptops will already be loaded with the database and other files.

<u>Option 2:</u>
This option works best when the students are conversant in loading software on their laptop, have the necessary minimum requirements on their laptop, and have administrator rights for loading software. The instructor will provide a CD to each student as part of the course handouts. The CD contains the install wizard programs to install the database on the laptop. It also contains other files to illustrate the user interface, input, and functions of the database.

As the instructor presents the instruction unit, the student will follow on their laptop so that at the end of the instruction block the student has an initial familiarization of the database features, how to use the database as a risk assessment/risk management tool, and has it loaded on the laptop for their personal use in the future.

It the student does not have a laptop, they may look over the shoulder of someone who does have a laptop or just follow along the slide presentation which uses screen captures of the software throughout the processes demonstrated.

Option 3:
When few students have laptops, the laptop users do not have administrator rights, or laptop users have other restrictions on loading new software, the demonstration / performance approach becomes too time consuming and detracts from the learning experience of most of the students. In this case, presentation of the PowerPoint visuals without demonstration / performance is the approach to use. Then at an identified time on Day 2, those who want to load the software on their laptops can do so with the help of the instructors. The instruction unit flows more smoothly in this situation and software loading problems only impact those who are loading the software.

Unit VII (C)

COURSE TITLE

Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer

TIME 75 minutes

UNIT TITLE

Explosive Blast

OBJECTIVES

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

SCOPE

The following topics will be covered in this unit:

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

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 4
2. Case Study – Appendix C: COOP, Cooperville Information / Business Center
3. Student Manual, Unit VII (C) (info only – not listed in SM)
4. Unit VII (C) visuals (info only – not listed in SM)

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
2. Instructor Guide, Unit VII (C)
3. Student Manual, COOP Case Study (C) (one per student)
4. Overhead projector or computer display unit
5. Unit VII (C) visuals, including E155_Unit07_Manchester.mpg which must be in the same electronic folder as the Unit VII visuals -- E155_Unit07 (C).ppt

UNIT VII (C) OUTLINE

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, Units IX, Site and Layout Design Guidance, and X, Building Design Guidance are excellent opportunities to illustrate the concepts in this instruction unit as applied to the Local Area.

- **Optional Activity:** There are no optional activities in this unit.

- **Additional Information COOP Case Study:** Figures 10, 11, and 12 in Appendix C: COOP, Cooperville Information / Business Center use the following information to obtain the radius (in feet) of the rings.
  Using FEMA 426, Figure 4-5, page 4-11:
    Structural damage -- Threshold, Concrete Columns Fail curve
    Probable lethal injuries -- Potentially Lethal Injuries curve
    Severe injuries from glass -- Glass with Fragment Retention Film – Severe Wounds curve
  Approximate Weapon Yield used:
    Figure 10 – 135 pounds TNT equivalent
    Figure 11 – 20,000 pounds TNT-equivalent
    Figure 12 – 1,000 pounds TNT equivalent.

- **Activity:** The students will answer questions in the Student Activity exercise using the range-to-effects chart and estimated pressures chart in FEMA 426 to evaluate stand-off distances and expected damage for selected questions and to identify the Design Basis Threat for this Case Study and determine stand-off distances for the same damage.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page (Unit #) in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- 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 a different student forward to the screen to answer the questions associated with each chart, including the Case Study values if time permits.

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

- Ask for and answer questions.

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

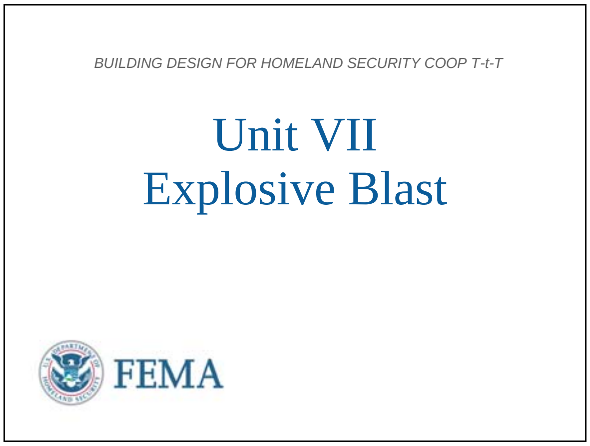
(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VII-C-1



Introduction and Unit Overview

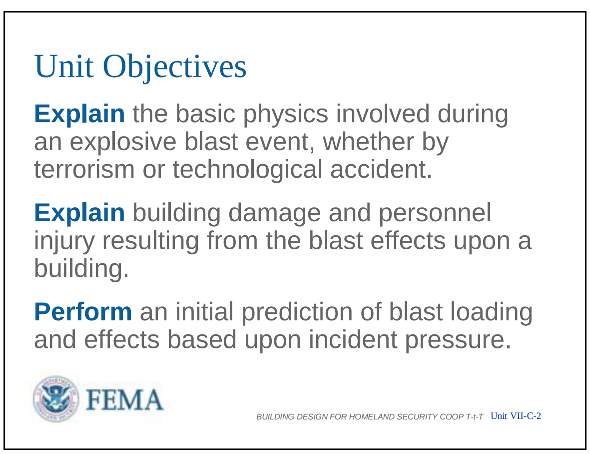
This is Unit VII Explosive Blast. Note that we are covering **pages 4-1 to 4-20 in FEMA 426** during this unit.

In the previous units, we determined the various initial ratings during the assessment process.

In this unit, we will examine how explosive blast impacts buildings and people to better understand the design recommendations and mitigation options presented in later units.

NOTE to instructor: Emphasize that the goal of this COOP unit is not to turn the students into blast experts. The students will be able to accomplish a GO / NO GO initial screening to determine if everything is OK or additional blast analysis is needed. The students will also understand the terminology and if a risk assessment has adequately covered explosive blast.

VISUAL VII-C-2



Unit Objectives

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

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VII-C-3

Unit VII: Explosive Blast

Units I-VI covered the Risk Assessment Process

Units VII and VIII explain Explosive Blast, CBR Agents, and their effects

Units IX and X demonstrate techniques for site layout and building design to counter or mitigate manmade threats and similar technological hazards

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VII-C-3

Explosive Blast

So far we have looked at the risk assessment process with the level of understanding achieved from the instruction yesterday.

Today we go into the technical basics of Explosive Blast and CBR agents to understand their effects and the benefit of their associated mitigation measures.

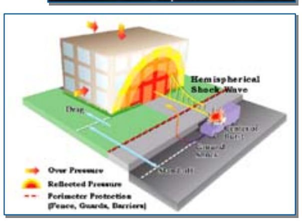
Then we will look at Site and Layout Design and Building Design mitigation measures for these terrorist tactics and similar technological hazards.

VISUAL VII-C-4

Blast Loading Factors

Explosive properties

- Type
- Energy output (TNT equivalency)
- Quantity



FEMA 427, Figure 2-1: Schematic of Vehicle Weapon Threat Parameters and Definitions, p. 2-2

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

<u>Pressure TNT equivalency</u> can generally range from <u>0.14 to 1.7</u>. If the pressure TNT equivalency is above 1.0, this means the explosive achieves a higher pressure (pressure equivalency) than TNT.

Blast Loading Factors

Explosive properties types – Is it a high explosive, medium explosive, or low-order explosive?

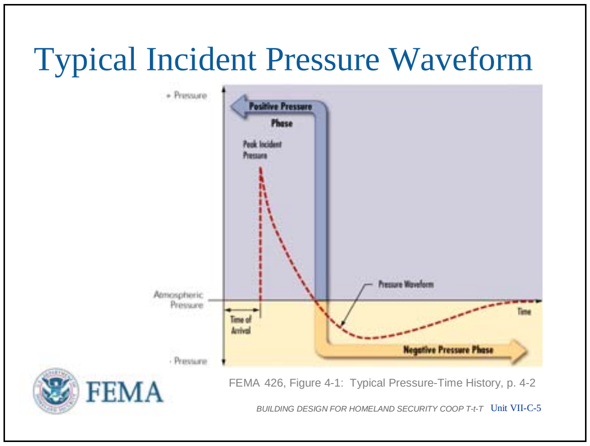
Is it specifically designed for the purpose – military grade explosive (C4, landmine, etc.) or a combination of generally available materials (ANFO, black powder)?

The energy output of explosives can be related by TNT (trinitrotoluene) equivalency. TNT equivalency is usually considered to be the relative pressure achieved by the explosive compared to what TNT can achieve.

Aside from TNT equivalency, the <u>larger the quantity of an explosive, the higher the pressures and the larger the impulse</u>.

INSTRUCTOR NOTES

VISUAL VII-C-5



NOTE to instructor: From a COOP standpoint, understanding the pressure waveform provides better understanding of how the blast wave interacts with the building, providing a basic understanding of damage and protection.

CONTENT/ACTIVITY

Typical Incident Pressure Waveform

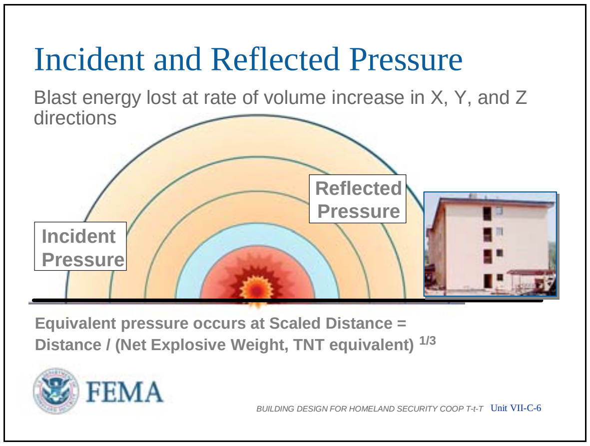
The explosive detonation generates a bubble of air moving at supersonic speed from the bomb location. <u>About one-third of the explosive material contributes to the detonation.</u>

As it reaches a point in space, such as a person or building, the pressure goes rapidly from atmospheric to peak pressure in very little time. The pressure at this point decays rapidly as the supersonic bubble moves on, its pressure reducing exponentially as the surface area of the bubble increases, expending energy over an ever increasing area. The pressure also drops off due to the completion of the chemical reaction of the explosive mixture (burning of the remaining two-thirds of the material). If the explosion occurs within a <u>confined space</u>, the gases generated by the burning of the explosive are contained and keep the pressure elevated over a longer period of time. [Indicate a longer tail off of the positive phase to illustrate the confined space variation.] Design is typically based on positive pressures.

The <u>negative phase</u> of the blast wave is the ambient air rushing in behind the blast wave to return to a stable pressure. Although the negative phase has much less energy than the positive phase, it can hit the structure at the most inopportune moment in its vibration, resulting in unexpected consequences – increased damage or having windows blow OUT of the building rather than into it.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

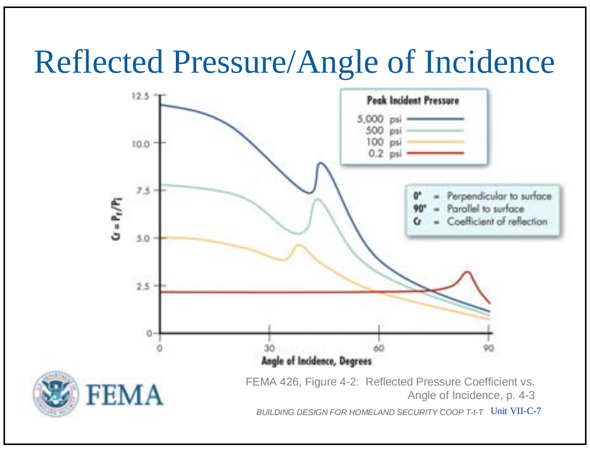
VISUAL VII-C-6



Incident and Reflected Pressure

When the incident pressure wave impinges on a structure that is not parallel to the direction of the wave's travel, it is reflected and reinforced. The reflected pressure is always greater than the incident pressure at the same distance from the explosion, and varies with the incident angle.

VISUAL VII-C-7



NOTE to instructor: Thus the reflected pressure is actually what causes the damage and keeping the reflected pressure in the 2.5 Coefficient of Reflection range is the reason why sufficient stand-off is so beneficial.

Reflected Pressure versus Angle of Incident

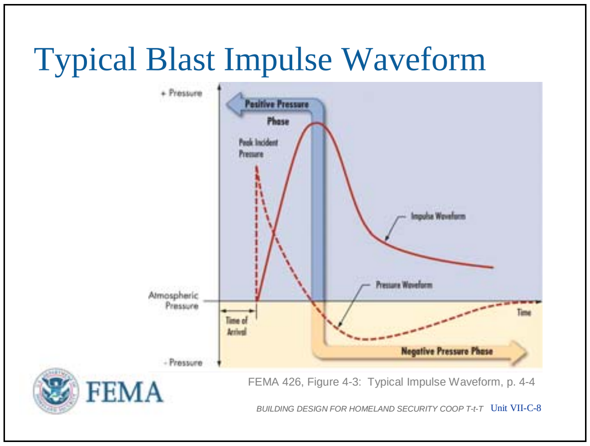
When the blast wave strikes an immovable surface, the wave reflects off the surface, resulting in an increase in pressure. This reflected pressure actually causes the damage to the building. A very high reflected pressure may punch a hole in a wall or cause a column to fail, while a low reflected pressure will try to push over the whole building.

The worst case is when the direction of travel for the blast wave is perpendicular to the surface of the structure and the incident pressure is very high. The <u>Coefficient of Reflection</u> can be <u>greater than 12</u> for high incident pressures.

By keeping the incident pressure low (by limiting the size of the explosive, maintaining a large distance between the explosive and the building, or both), the reflected pressure can be kept low. Keeping the <u>Coefficient of Reflection below 2.5</u> by keeping the peak incident pressure below 5 psi (pounds per square inch) is a desirable goal.

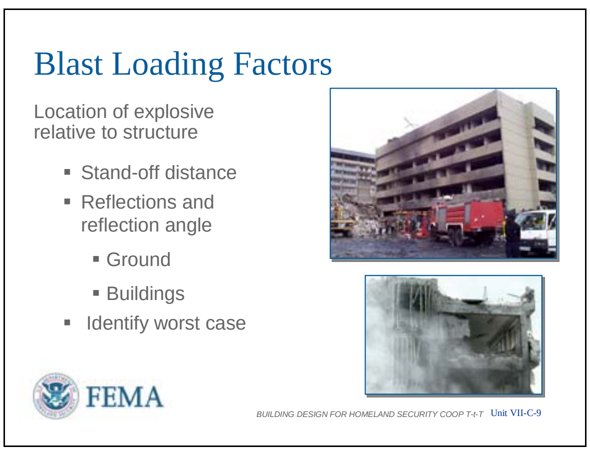
INSTRUCTOR NOTES

VISUAL VII-C-8



There is also a TNT equivalency based upon impulse and that ranges from 0.5 to 1.8. If the impulse TNT equivalency is above 1.0, then the explosive has a longer push (impulse equivalency) than TNT.

VISUAL VII-C-9



CONTENT/ACTIVITY

Typical Blast Impulse Waveform

Another consideration is the impulse of the blast wave, which is the integration of the peak incident pressure (both positive phase and negative phase) at the point in question over time.

A general rule of thumb:

- Brittle materials (like glass) respond to peak incident pressure and are less affected by impulse. Thus a high order explosive with high incident pressure will easily damage glass.
- Ductile materials (like most building structures), on the other hand, respond more to impulse (the total push) rather than peak incident pressure (the maximum hit). Thus, a low order explosive with a large impulse that pushes for a longer time will cause more damage to buildings.

Blast Loading Factors

Location Relative to Structure: Stand-off distance is your best friend. The larger the distance between the explosive and the structure:

- The lower the incident pressure and
- The lower the resultant reflected pressure.

We will investigate this in more detail later.

As we have already seen, the reflection angle at which the blast wave strikes the structure also affects the value of reflected pressure.

The ground is also a reflection surface to consider.

- If the bomb is placed close to the ground, the ground reflection adds a small amount of incident pressure to the situation.
- If the bomb is elevated (a more difficult task), the ground reflection can become

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

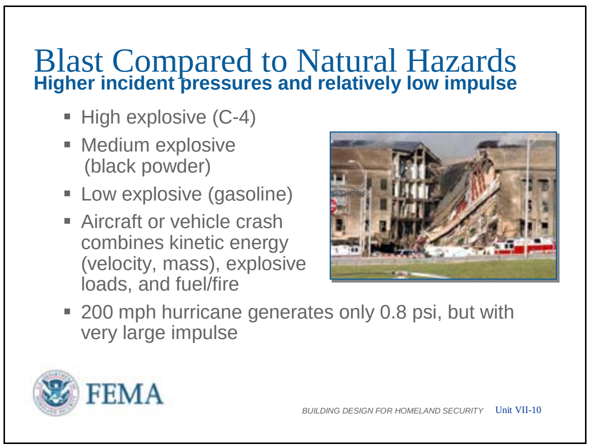
significant, but the reflection off the building surface diminishes.

Identifying the worst case situation begins by finding the:

- Closest approach (stand-off distance) between the explosive and the building
- Then consider the angle of reflection.

Or put another way – place the explosive directly perpendicular to the largest face of the building, with the explosive centered upon the building's face as close as you can get.

VISUAL VII-C-10



Low explosive (or Combustion explosive) – sustained combustion, usually of gases or fine dust – natural gas, gasoline, flour, coal dust

Medium explosive (or Low-Order Velocity explosive) – deflagration (subsonic [slower than speed of sound] combustion propagating through the explosive material by hot burning material heating next layer of cold material and igniting it) – contained black powder, smokeless powder, propellants, pyrotechnics

Low and medium explosives have burning velocities of less than 3,300 feet per second and generate a subsonic explosion without an

Blast Compared to Natural Hazards

There are a number of similarities between blast loading and building response in comparison to building response from earthquake, flood, or wind loading, but there are also significant differences.

- Low and medium explosives generate less pressure than high explosives, but the low & medium explosive impulse can last longer than the high explosive impulse (in the range of hundreds of milliseconds versus tens of milliseconds).
- Blast loads are high amplitude, low duration (milliseconds) events that create an air pressure wave that acts over the entire building envelope. They have relatively low impulse whether high or low explosives compared to natural hazards.
- Earthquake loads are usually low amplitude, high-energy, long-duration (seconds) events that are transferred through the foundation.
- Flood loading has high-energy, relatively high amplitude, and very long duration loading (minutes) that impact everything in its path with increased reflected pressures and extensive damage. The higher the velocity of the flood waters coupled with the increased mass of water results in extensive damage.

INSTRUCTOR NOTES

overpressure wave. Note that the speed of sound at 77^{o}F is 1,137.3 feet per second.

High explosive (or High-Order Velocity explosive) – detonation (supersonic [faster than the speed of sound] combustion in which a shock wave compresses the material thus increasing the temperature to the point of ignition – C-4, TNT, ANFO (ammonium nitirate – fuel oil)

High explosives burn at speeds above 3,300 feet per second and generate a supersonic explosion with a blast wave.
C4 burn rate – 26,000 feet per second
ANFO burn rate – 8,000 feet per second

VISUAL VII-C-11

Many of the mitigation options for seismic and hurricane retrofit such as moment connections, elimination of progressive collapse, laminated glass, and strengthened architectural elements mitigate many explosive blast vulnerabilities.

CONTENT/ACTIVITY

- High winds are dynamic and typically affect the envelope, but are of low amplitude compared to blast. However, they push for a very long time (in the range of seconds or longer) and, thus, have very large impulse. (Note: wind gusts are rated for 3 seconds duration minimum, but sustained winds can push for minutes.).
- A nuclear blast or millions of pounds of high explosives would generate high pressures AND long duration impulse (in the range of seconds).

Blast Compared to Natural Hazards

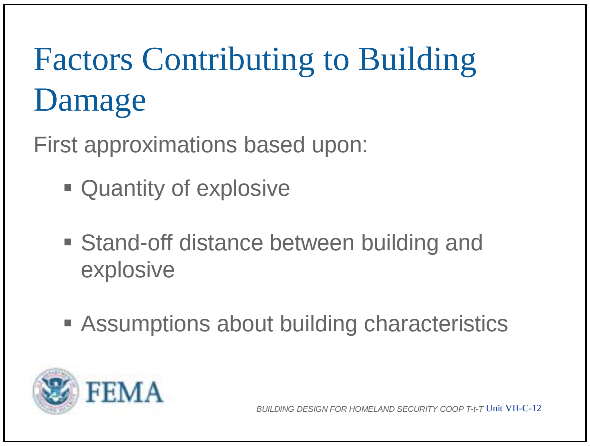
Explosive blast tends to cause localized damage compared to other hazards that may destroy the whole building.

- The first building surface struck will get the greatest pressures, and expect it to receive the greatest damage. The blast may break a building component by punching through it (window or wall) or shearing it (column).
- The other side of the building, due to its greater distance from the explosion, will see lower pressures, unless there are nearby buildings that will reflect the blast wave back to the building in question.
- Reflections can increase damage to the building, but are hard to quantify.
- Greater mass has usually been the design of choice to protect against explosive blast. The inertia of the mass slows the structural reactions to the point that the impulse is over before the building tends to move.
- Conversely, additional mass is usually undesirable during an earthquake due to the long duration, low frequency forces

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

that can get the mass moving. Earthquake design usually concentrates on lighter structures with great ductility and additional reinforcement at weak points.

VISUAL VII-C-12
HIDDEN SLIDE



Factors Contributing to Building Damage

Certain prediction of damage to buildings and people during an explosive event is beyond the scope of the reference manual. There are too many variables that would have to be considered and modeling would take many months for analysis by supercomputer. Thus, as in standard building design, we use approaches with safety factors that provide adequate first approximations to estimate response based upon the:

- The amount of explosive usually expressed as TNT equivalent weight.
- The stand-off distance between the explosive and the building or person.
- Assumptions about building characteristics – the exterior envelope construction (walls and windows) and the framing or load-bearing system used.
- The building characteristics provide insight into weaknesses and allow general predictions about how the building will respond.

VISUAL VII-C-13

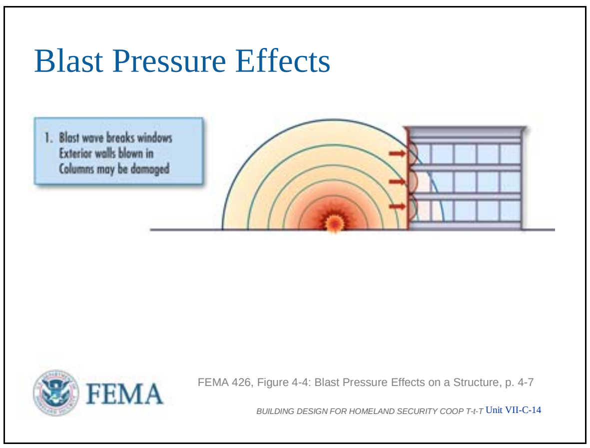
Types of Building Damage

- Direct air blast, especially from close-in explosions, results in component failure of walls, windows, columns, and beams / girders.
- The pressures experienced by the building can far exceed the building's original design and can occur in directions that were not part of the original design.
- Once the exterior envelope is breached, the blast wave causes additional structural and non-structural damage inside the building.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

- Collapse, which is covered in more detail in **Chapter 3 of FEMA 426**, is a primary cause of death and injury in an explosive blast if it occurs.
- Localized collapse may have a load-bearing wall, or portion thereof, on one side of the building fall to the ground or a single column fails and the surrounding floors fall with it.
- Progressive collapse is more disastrous as a single component failure, like a wall or column, results in the failure of more walls and columns so that more of the building falls to the ground than what the explosive initially affected.

VISUAL VII-C-14

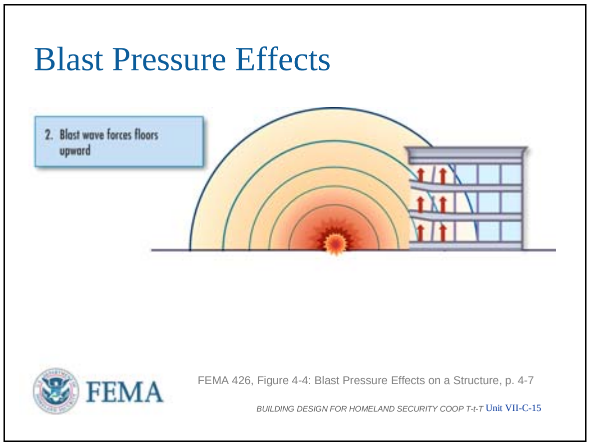


Blast Pressure Effects (1 of 3)

- The air blast strikes the exterior wall and the weakest component will fail first – usually the windows, which saves the walls and columns, but causes much non-structural damage inside the building.
- Note that unreinforced masonry walls can be weaker than windows, especially if they are non-load bearing.
- If the explosive is close enough, the walls can breach and one or more columns can fail in addition to the windows.
- Based upon the reflection angle, one can expect the lowest or lower floors (1 to 3) to receive the greatest damage.
- If the blast wave strikes the whole surface of the exposed side simultaneously, this is called a laminar situation, and breaching (puncture) of walls and failure of columns is less likely. This is what is sought by achieving a large stand-off distance.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

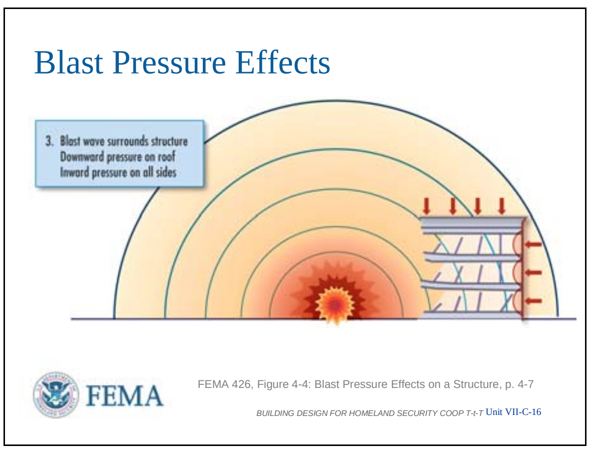
VISUAL VII-C-15



Blast Pressure Effects (2 of 3)

- Once the blast wave enters the building, it is trapped and more air enters the building, further increasing the pressure. Structural components like flooring and shear walls now are moving in directions for which they were not designed.
- Floor failure can result in three effects:
  - o Concrete chunks raining down, causing injury and possibly death
  - o Whole floor gives way and pancakes downward with obviously more serious consequences
  - o If flat slab construction is present (thickened floors act as beams in the framing system), the floors can disconnect from the columns, resulting in floor AND column failure.

VISUAL VII-C-16

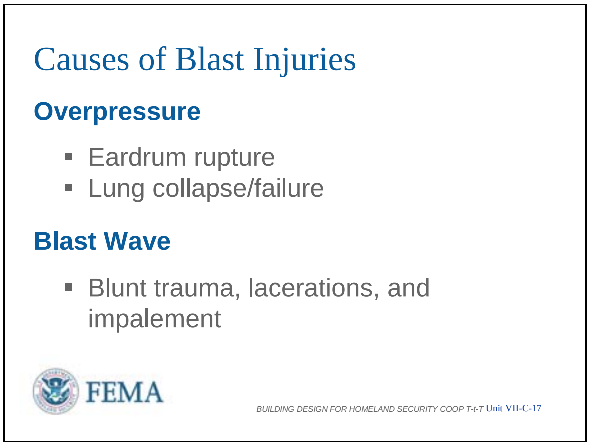


Blast Pressure Effects (3 of 3)

- The blast wave continues to engulf the building. Any building component that traps the blast wave, like an overhanging roof, can expect increased damage, based upon how it is constructed and attached.
- The roof and sides parallel to the blast wave movement will see incident pressure only, which should result in little or no damage.
- Once the blast wave has passed the building, the far side (opposite the side first experiencing the blast wave) will see increased pressure as a slight vacuum forms and the ambient air rushes back in to achieve equilibrium. Reflections of the blast wave off other buildings behind this one can also increase the pressure impinging the far side.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

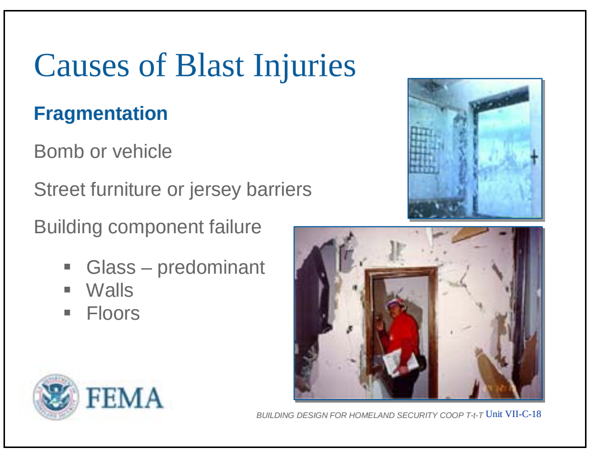
VISUAL VII-C-17



Causes of Blast Injuries

- Injuries and casualties occur in three ways during explosive blast by:
  - Overpressure
  - Motion of person by blast wave
  - Fragmentation generated by blast wave
- Overpressure causes eardrum rupture first, which is normally not lethal.
- Overpressure can also overdrive the lungs, causing injury or death. The relationship between pressure and impulse is very evident in lung response. An incident pressure of 102 psi for 3 milliseconds is the threshold of lethality as is an incident pressure of 23 psi for 18.5 milliseconds.
- Blunt trauma, lacerations, and impalement injuries occur when the blast wave picks up the person and throws them against a surface or object (translation), or glass and wall fragments cause lacerations or blunt trauma on impact. In relative distance terms, death by translation occurs at a greater distance for the same bomb size than death by lung overpressure.

VISUAL VII-C-18



Causes of Blast Injuries

- Fragmentation from any source can result in blunt trauma, impact, and penetration, or laceration injuries.
- The fragments can come from around the bomb or from parts of the vehicle.
- They can be picked up either intact or damaged by the blast wave as it travels along – street furniture or jersey barriers.
- Building component failure also causes material fragments with sufficient velocity to injure or kill. Note that upward of 80 percent of all injuries from explosive blast can be attributed to lacerations caused by broken glass. The most effective way to reduce injuries during explosive blast is harden the glass and window frame system and/or reduce the amount of glass.

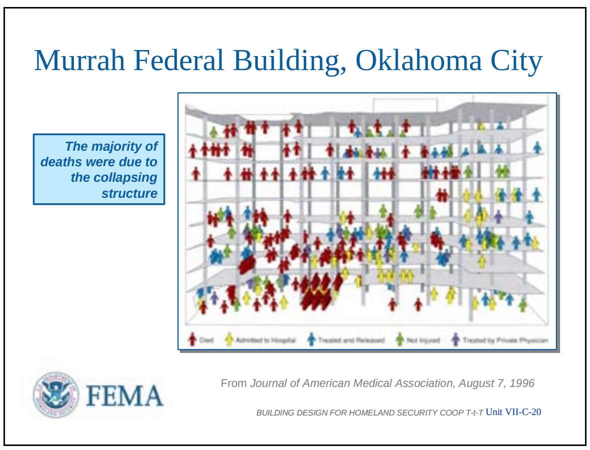
INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL VII-C-19

Murrah Federal Building

The Murrah Federal Building is typical of many commercial properties in the current inventory. The bomb was designed as a shape charge and detonated in the drop-off area, destroying two primary columns and causing the spandrel beam to rotate. The floors above failed in progressive collapse and the blast wave penetrated deeply into the interior.

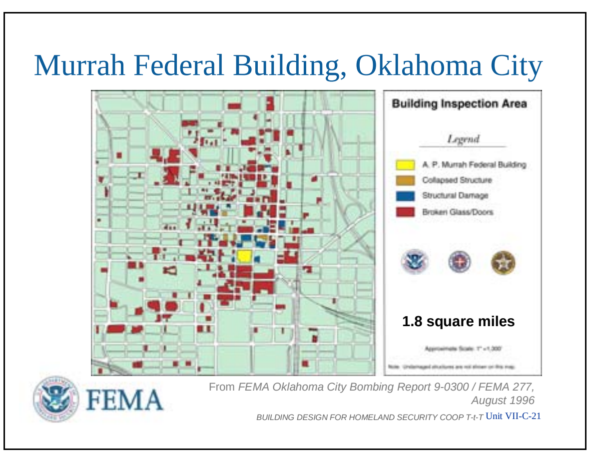
VISUAL VII-C-20



Murrah Federal Building

The majority of deaths were caused by the collapsing structure.

VISUAL VII-C-21



Murrah Federal Building

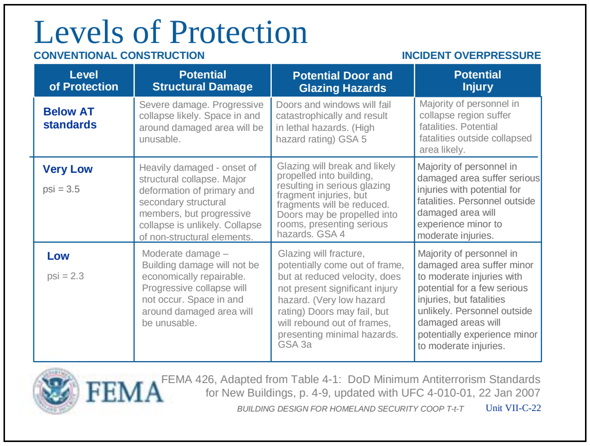
The collateral damage zone extended out several thousand feet, with extensive glass and debris injuries.

Glass was broken as far as 0.9 miles away.

NOTE: The map is approximately <u>1.35 miles on a side.</u>

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VII-C-22


Levels of Protection

CONVENTIONAL CONSTRUCTION — INCIDENT OVERPRESSURE

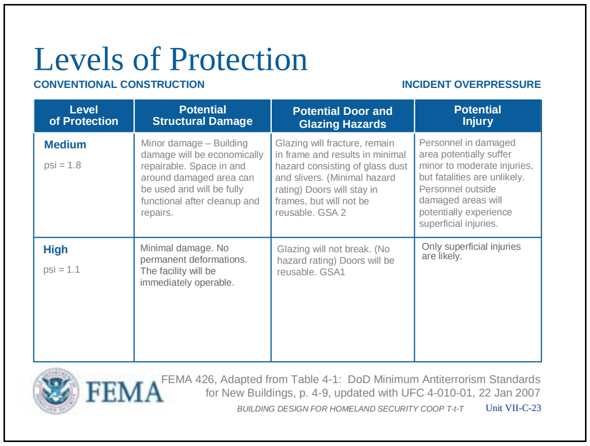
Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Below AT standards	Severe damage. Progressive collapse likely. Space in and around damaged area will be unusable.	Doors and windows will fail catastrophically and result in lethal hazards. (High hazard rating) GSA 5	Majority of personnel in collapse region suffer fatalities. Potential fatalities outside collapsed area likely.
Very Low psi = 3.5	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 likely propelled into building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards. GSA 4	Majority of personnel in damaged area suffer serious injuries with potential for fatalities. Personnel outside damaged area will experience minor to moderate injuries.
Low psi = 2.3	Moderate damage – Building damage will not be economically repairable. Progressive collapse will not occur. Space in and around damaged area will be unusable.	Glazing will fracture, potentially come out of frame, but at reduced velocity, does not present significant injury hazard. (Very low hazard rating) Doors may fail, but will rebound out of frames, presenting minimal hazards. GSA 3a	Majority of personnel in damaged area suffer minor to moderate injuries with potential for a few serious injuries, but fatalities unlikely. Personnel outside damaged areas will potentially experience minor to moderate injuries.

NOTE to instructor: This updated DoD Levels of Protection are taken from the UFC dated 22 January 2007.

Levels of Protection

- The Department of Defense (DoD) and the General Services Administration (GSA) call out similar levels of protection that relate building damage and potential injury. This slide and the next summarize these perspectives.
- **NOTE:** The GSA glass ratings and estimated incident pressure levels are added to the DoD UFC criteria as best meet the description for comparison.
- This slide represents the conventional construction found in most buildings.
- Note the relatively low values for incident pressure for each level of protection.
- The Low Level of Protection can be interpreted as the threshold of lethality and is a desirable minimum design goal to achieve. If the risk, such as the likelihood, of experiencing an explosive blast is high, consideration for use of a higher level of protection would be in order.

VISUAL VII-C-23
HIDDEN SLIDE


Levels of Protection

CONVENTIONAL CONSTRUCTION — INCIDENT OVERPRESSURE

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Medium psi = 1.8	Minor damage – Building damage will be economically repairable. Space in and around damaged area can be used and will be fully functional after cleanup and repairs.	Glazing will fracture, remain in frame and results in minimal hazard consisting of glass dust and slivers. (Minimal hazard rating) Doors will stay in frames, but will not be reusable. GSA 2	Personnel in damaged area potentially suffer minor to moderate injuries, but fatalities are unlikely. Personnel outside damaged areas will potentially experience superficial injuries.
High psi = 1.1	Minimal damage. No permanent deformations. The facility will be immediately operable.	Glazing will not break. (No hazard rating) Doors will be reusable. GSA1	Only superficial injuries are likely.

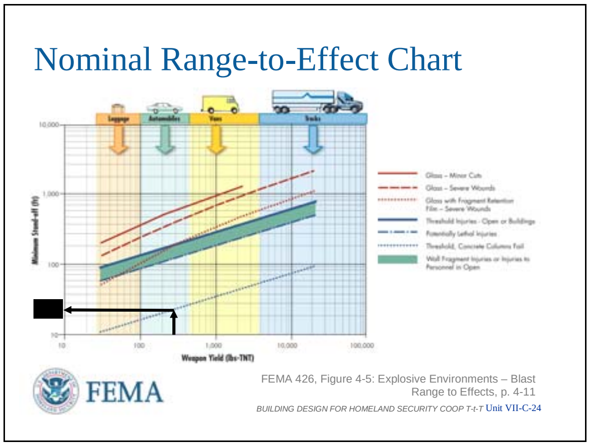
Levels of Protection

- When greater protection resulting in less damage and injury is desired, this slide indicates that the pressures must be kept low for conventional construction.
- Alternately, the building must be hardened to achieve these lower levels of damage and resultant injury. This is especially necessary when the incident pressure is higher due to the design basis threat explosive quantity being at a closer stand-off distance than conventional construction can handle.

<u>The building owner selects the Level of Protection and the Design Basis Threat, which in turn determines the stand-off distance required.</u>

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL VII-C-24



Direct students' attention to **Figure 4-5 on page 4-11 of FEMA 426**.

NOTE to instructor: Emphasize to COOP students that the desirable location on the Range-to-Effect chart is the upper left where the security measures will only allow small weapon yields and stand-off is great (above the uppermost curve indicating that even if the bomb goes off the stand-off reduces the blast loading to the point that little damage occurs).

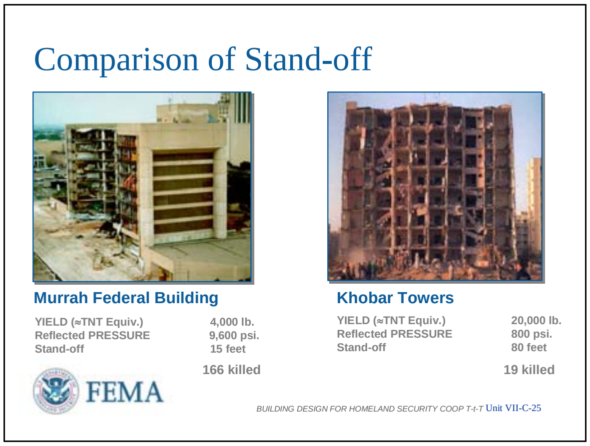
Nominal Range-to-Effect Chart

- The Nominal Range-to-Effect Chart is a handy way to represent the stand-off distance at which a given bomb size produces a given effect.
- If you are below the curve for the given effect, that effect has the potential to occur. The further below the curve, the more likely it will happen and the greater the expected damage.
- Conversely, an intersection point between range or stand-off distance and weapon yield or bomb size in TNT equivalent weight that is above the curve for the given effect indicates that there is a good chance that that effect will not occur. However, many variables can alter these curves, such as reflections, resulting in damage at a point above the curve.
- The chart also concentrates upon the two prominent concerns during explosive blast – glass injury and progressive building collapse. In most, but not all cases, the glass is the weakest component of the building envelope. Conversely, the columns, whether concrete or steel, are usually the strongest components of the building envelope. [A workable rule of thumb is that steel columns require about twice the stand-off distance compared to concrete columns for the same weapon yield.]

- **Question:** Ask what stand-off distance for a 300-pound (TNT-equivalent) bomb is needed to just exceed the threshold of concrete column failure?
    - **Answer:** Approximately 25 feet.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL VII-C-25



Comparison of Stand-off

The Murrah Federal Building and Khobar Towers vividly illustrate the response of a building to a blast event.

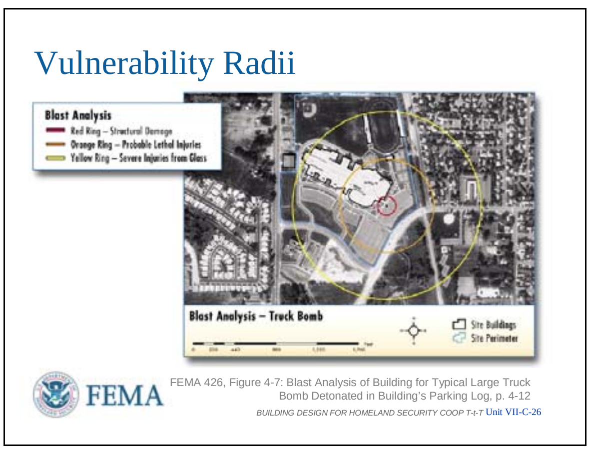
The Murrah Federal Building had less than 20 feet of stand-off and was not designed to prevent progressive collapse.

Khobar Towers was designed using British code to prevent progressive collapse and had approximately 80 feet of stand-off distance.

Notice the size of the weapons.

The Murrah Federal Building was unsalvageable and demolished, while Khobar Towers only lost the front façade and was restored and placed back into service.

VISUAL VII-C-26

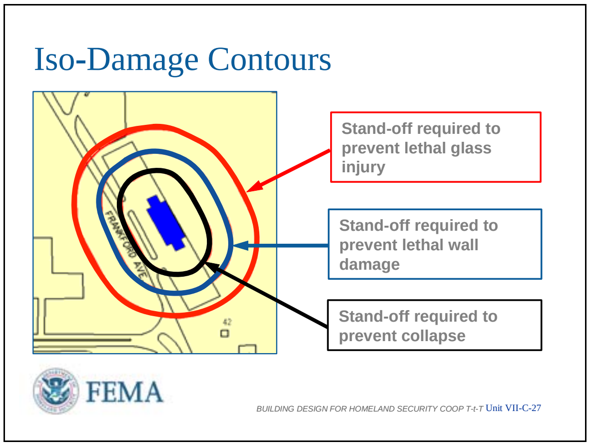


Vulnerability Radii

- Graphically portraying the information from the Nominal Range-to-Effect Chart can be done in two ways. As shown in **Figures 4-6 and 4-7 in FEMA 426 (page 4-12)**, vulnerability radii show how far a given type of damage will extend from a bomb location for a given weapon yield upon the building of interest for which the blast analysis was performed.
  - The rings indicate where that level of damage starts and whatever is inside the ring will experience that damage.
  - The expected damage increases as you move from the ring to the explosion.
  - Hardening and other mitigation measures can be compared using this representation (for example, existing glass, glass with fragment-retention film installed, or upgraded glass).
- This representation works well when showing the effects of different bomb locations and the extent of the building affected by that bomb.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

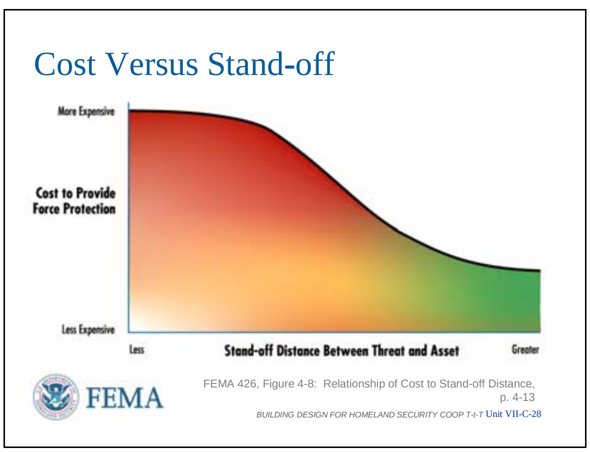
VISUAL VII-C-27



Iso-Damage Contours

- Alternately, the nominal range-to-effect information can be graphically represented as iso-damage contours. For a given weapon yield against a building of known construction, the contour indicates how far the bomb or vehicle must be kept away to prevent the damage indicated in this slide.
  - The intent here is to focus on the required stand-off distance to prevent or reduce the weapon effect portrayed by the contour.
  - Thus, to prevent structural collapse, vehicle parking should be eliminated or tightly restricted inside the black contour.
  - Likewise, to prevent lethal glass injury, the vehicle parking should be outside the red contour.

VISUAL VII-C-28



Cost versus Stand-off

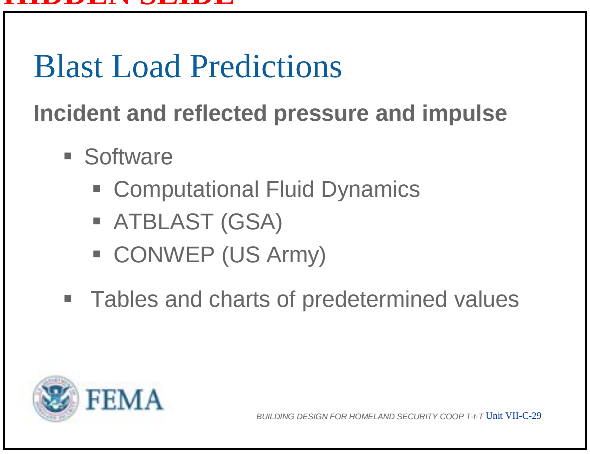
- As in any design for new construction or renovation, there are trade-offs that must be considered. Although increasing the distance between the closest approaches of a vehicle bomb to the building is highly desirable, it is not without a cost.
- The increased distance means more land is needed, which may require considerable time and expense to acquire. The increased land also means a larger perimeter boundary that then requires more perimeter fencing, landscaping, vehicle barriers, lighting, closed-circuit television, etc. Thus, while the increased stand-off allows a less expensive building to be constructed, there are other costs that must be considered in the overall project.
- Where stand-off distance cannot be increased, building hardening is usually necessary to achieve the same level of protection against the Design Basis Threat

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

weapon yield. As the stand-off distance decreases, the cost of hardening significantly increases because the building must now withstand damage that it would not experience at higher stand-off.

- Consider progressive collapse. At large stand-off distance, the design of the building framing and columns should meet basic design to prevent progressive collapse. This would be for the loss of one column, for example. At smaller stand-off distances, the columns may require additional hardening to prevent the failure of more than one column during an explosive blast event.

VISUAL VII-C-29
HIDDEN SLIDE

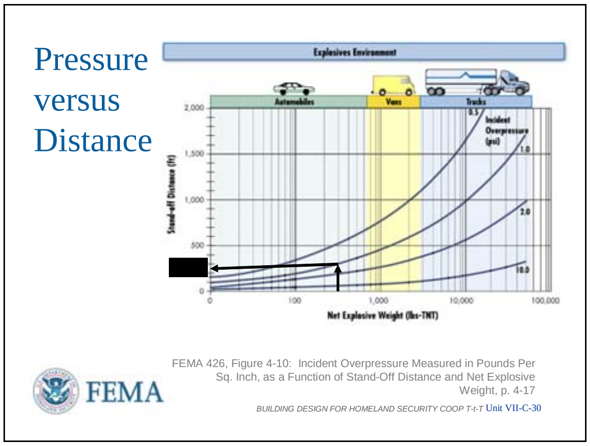


Blast Load Predictions

- The first step in designing a building for explosive blast is to understand the pressures and impulses the building may experience during the potential blast event.
  - If reflections are a concern, then high-level software, such as Computational Fluid Dynamics (CFD), may be in order.
  - Defense Threat Reduction Agency software (not CFD) – Vulnerability Assessment and Protection Option (VAPO) can handle reflections, but modeling takes much longer than simpler models and reflection analysis takes hours of computation time on a laptop.
  - As a first effort, simpler software, such as ATBLAST and CONWEP, can give a prediction of incident blast loading values and a prediction for reflected pressure and impulse using simplifying assumptions.
- Pressure versus distance **(Figure 4-10 in FEMA 426, page 4-17)** is another method for predicting the incident pressure as shown in the next slide.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VII-C-30



Direct students' attention to **Figure 4-10, page 4-17 of FEMA 426.**

NOTE to instructor: Just like the Range-to-Effect Chart, this graph is provided to allow an initial screening of a COOP facility to determine if explosive blast is a problem and whether or not additional analysis is required.

Pressure versus Distance

- Figure 4-10 breaks the blast load estimate into the essential elements of weapon yield or explosive weight in TNT equivalent on the x-axis and stand-off distance on the y-axis to give an incident pressure value that a building can experience.
- Note that the x-axis is logarithmic and the y-axis is linear. If both axes were logarithmic as used on the range-to-effect chart presented earlier, the curves of this chart would be straight lines. In other words, on a log-log scale of explosive weight and stand-off distance, a straight line indicates a pressure relationship (not impulse).
- **Question**: Ask what stand-off distance is required for a 300-pound bomb to keep the incident pressure at 1.0 psi or lower.
  - **Answer:** Approximately 250 feet.

VISUAL VII-C-31
HIDDEN SLIDE

Blast Damage Estimates

Assumptions - pressure and material

- Software - SDOF
  - AT Planner (U.S. Army)
  - BEEM (TSWG)
  - BlastFX (FAA)
- Software - FEM
- Tables and charts of predetermined values

FEMA

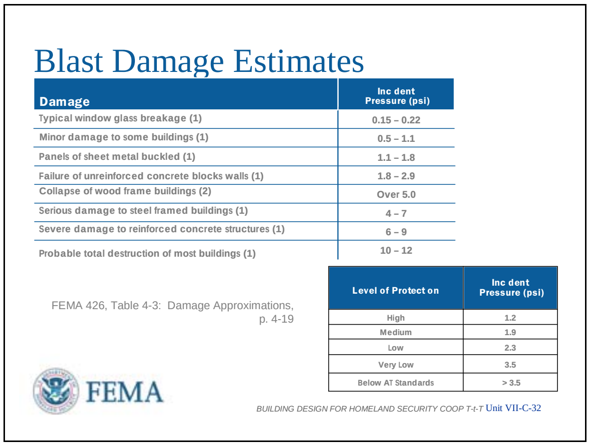
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VII-C-31

Blast Damage Estimates

- Whereas normal design usually uses constant loading and linear response, blast loading is very dynamic, as you have seen, and damage of building components enters its nonlinear material range prior to failure.
- SDOF (Single Degree of Freedom) software allows initial simplified dynamic analysis
- Conversely, higher level modeling may result in reduced construction costs due to a better understanding of how the building components will respond during a blast for the given site, layout, and building design parameters selected. This is balanced by the additional cost of the higher level modeling.

INSTRUCTOR NOTES

VISUAL VII-C-32

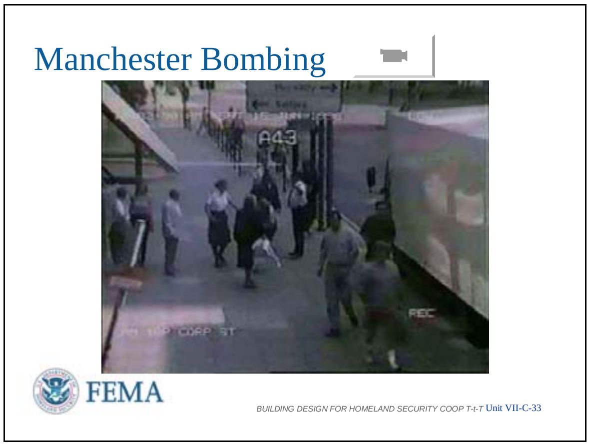


Damage	Inc dent Pressure (psi)
Typical window glass breakage (1)	0.15 – 0.22
Minor damage to some buildings (1)	0.5 – 1.1
Panels of sheet metal buckled (1)	1.1 – 1.8
Failure of unreinforced concrete blocks walls (1)	1.8 – 2.9
Collapse of wood frame buildings (2)	Over 5.0
Serious damage to steel framed buildings (1)	4 – 7
Severe damage to reinforced concrete structures (1)	6 – 9
Probable total destruction of most buildings (1)	10 – 12

Level of Protect on	Inc dent Pressure (psi)
High	1.2
Medium	1.9
Low	2.3
Very Low	3.5
Below AT Standards	> 3.5

NOTE to instructor: With the previous incident pressure chart a quick screening allows a COOP assessor or manager to have a basic understanding of the vulnerability of a COOP facility to explosive blast.

VISUAL VII-C-33



NOTE to instructor: Ensure the video file (**L156_Unit07_Manchester.mpg**) is in the same folder as the PowerPoint presentation to have the camera link after the slide title to work.

QUESTION: Ask students -- How big do

CONTENT/ACTIVITY

Blast Damage Estimates

- In this slide, you see Damage Approximations for different types of damage and a range of incident pressures at which this damage is expected to occur.
- Note that, logically, higher pressure results in greater damage and the range of incident pressure indicates the construction variation that may be found.

NOTE to instructor: **Table 4-3 on page 4-19 of FEMA 426** is based upon information from the following publications:

- "*Explosive Shocks in Air*" Kinney and Grahm, 1985
- *"Facility Damage and Personnel Injury from Explosive Blast"* Montgomery and Ward, 1993
- *"The Effects of Nuclear Weapons, 3rd Edition",* Glasstone and Dolan, 1977

Manchester Bombing

General Points to make as the video runs

- The truck was parked at about 9:20am, and the bomb exploded just under 2 hours later. The blast was audible over 8 miles away.
- Irish Republican Army gave advance notification at about 1 hour prior to detonation to newspapers, radio stations, and at least one hospital
- The police began clearing the street 40 minutes before the blast, but people still walk past the suspected truck at 17 minutes prior to the explosion.
- British Telecom has a special terrorist pager that identifies location and time in order to notify building occupants of the situation and direct evacuation routes
- This is the High Street of Manchester – the center of the city's business district at 10 AM on a Saturday morning just before Father's Day

INSTRUCTOR NOTES

you think this bomb was?
Answer: Reported to be 3,300 pounds but not stated as either actual weight or TNT equivalent. The bomb smashed almost every window in a half-mile radius.

Even with the advance notification Manchester's ambulance services counted 206 injured people (NO DEATHS). Most injuries were sustained from falling glass and building debris. In the immediately ensuing chaos, ambulances and private cars were used to shuttle victims to local and regional hospitals.

The majority (129, 62%) of casualties sustained minor injuries from flying glass. A significant number of casualties (36, 18%) presented with emotional distress or medical problems. A wide age range of casualties was involved. Few patients (19, 9%) required admission to hospital. There were no deaths and no casualties sustained major trauma.

VISUAL VII-C-34

Summary

Explosive blast physics

Blast damage to buildings

Injury to personnel

Prediction of loading, damage, and injury

- Range-to-effect chart
- Incident pressure chart

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VII-C-34

CONTENT/ACTIVITY

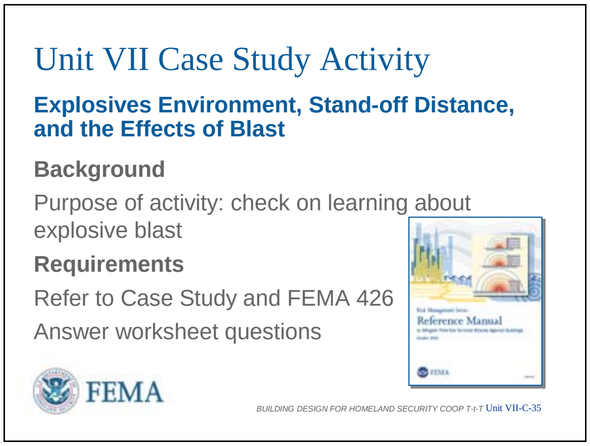
- Note that the High Street of many British cities are well covered by CCTV
- The double line on the street by the curb means no parking, thus making the truck suspicious -- as nothing was being off-loaded or on-loaded.
- Robot sent in to identify the bomb and possibly disarm it, but without success
- Bomb goes off with a great noise, then the explosion is shown in slow motion – note the 1/3 of the explosive providing the supersonic shock wave followed by the 2/3 of the explosive adding to the blast wave but also supporting the fireball through the conflagration (burning)
- Note the amount of debris, that NO buildings collapsed, that SOME walls remained intact, that ALMOST ALL glass was shattered, with damage being reduced the further the building was from the bomb
- The Post Office box, looks like a single heavy bollard survived the blast and has a commemorative plaque installed
- Prior to the bombing the Manchester High Street was quickly going down hill, but after the bombing there was a big influx of investment, and after 4 years of reconstruction the High Street is now among the best in Great Britain.

Summary

- You now have an understanding of the basic physics involved during an explosive blast event.
- You can now explain building damage and injury to people resulting from the blast effects upon a building and injury to people in the open.
- You can perform an initial prediction of blast loading and effects based upon incident pressure using a nominal range-to-effect chart or the incident pressure charts.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VII-C-35



Student Activity

This activity provides a check on learning about explosive blast.

Activity Requirements

Working in your small groups, refer to **FEMA 426** and complete the worksheet questions in the Unit VII Case Study activity in the Student Manual.

After 10 minutes, solutions will be reviewed in plenary group. This is a good opportunity to select two members of the class to go to the screen and answer the questions using the charts.

Transition

Unit VIII will cover CBR measures and introduce the basic science needed to understand building protection against chemical, biological, and radiological agents. Unit IX will begin the process of reviewing the site, layout, and building design guidance, further vulnerability assessment, and recommended mitigation options.

This page intentionally left blank

UNIT VII (C) CASE STUDY ACTIVITY:
STAND-OFF DISTANCE AND THE EFFECTS OF EXPLOSIVE BLAST
(COOP Version)

The requirements in this unit's activity are intended to provide a check on learning about explosive blast and understand the impacts of the Case Study's Design Basis Threat.

Requirements

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

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

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

   - What is the minimum stand-off distance from explosion of a 100-pound (TNT equiv.) bomb to have a level of confidence that severe wounds from glass (without fragment retention film) will not occur? ***270 feet***

   - What damage will be sustained at 400 feet from a 5,000-pound (TNT equiv.) explosion? ***Wall fragment injuries or injuries to personnel in the open and all curves above that point -- glass injuries ranging from minor cuts to severe wounds, with or without fragment retention film.***

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

   - What is the minimum stand-off required to limit the incident pressure to under 0.5 psi for a 100-pound (TNT equiv.) bomb? ***Approximately 325 feet***

   - What incident pressure would be expected at 500 feet from a 500-pound (TNT equiv.) bomb and what is the approximate damage? ***Approximately 0.75 psi, minor damage to some buildings or severe wounds from broken glass***

4. Refer to **Figure 4-5 (page 4-11) in FEMA 426** to answer the following questions.

- For the Design Basis Threats of the selected Case Study being used in this course offering, determine the standoff distance for the damage or injury indicated:

  - ________ pounds TNT-equivalent
    - Glass – Severe Wounds – ______ feet
    - Potentially Lethal Injuries – ______ feet
    - Threshold, Concrete Columns Fail – ______ feet

  - ________ pounds TNT-equivalent
    - Glass – Severe Wounds – ______ feet
    - Potentially Lethal Injuries – ______ feet
    - Threshold, Concrete Columns Fail – ______ feet

  - ***250 pounds TNT-equivalent (suburban)***
    - ***Glass – Severe Wounds – 400 feet***
    - ***Potentially Lethal Injuries – 125 feet***
    - ***Threshold, Concrete Columns Fail – 23 feet***

  - ***5,000 pounds TNT-equivalent (suburban and urban)***
    - ***Glass – Severe Wounds – 1,310 feet***
    - ***Potentially Lethal Injuries – 320 feet***
    - ***Threshold, Concrete Columns Fail – 60 feet***

Unit VIII (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 75 minutes
UNIT TITLE	Chemical, Biological, and Radiological (CBR) Measures
OBJECTIVES	1. Explain the five possible protective actions for a building and its occupants. 2. Compare filtration system efficacy relative to the particles present in CBR agents. 3. Explain the key issues with CBR detection. 4. Identify the indications of CBR contamination.
SCOPE	The following topics will be covered in this unit: 1. Five protective actions for a building and its occupants: evacuation; sheltering in place; personal protective equipment; air filtration and pressurization; and exhausting and purging. 2. Air filtration and cleaning principles and its application. 3. CBR detection technology currently available. 4. Indications of CBR contamination that do not use technology.
REFERENCES	1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 5 2. FEMA 426, *Appendix C*, Chemical, Biological, and Radiological Glossary 3. FEMA 453, *Design Guidance for Shelters and Safe Rooms,* Chapters 1 and 3 4. Case Study – Appendix C: COOP, Cooperville Information / Business Center 5. Student Manual, Unit VIII (C) (info only – not listed in SM) 6. Unit VIII (C) visuals (info only – not listed in SM)
REQUIREMENTS	1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Building*s (one per student) 2. Instructor Guide, Unit VIII (C) 3. Student Manual, COOP Case Study (C) (one per student) 4. Overhead projector or computer display unit

5. Unit VIII (C) visuals
6. Chart paper, easel, and markers (one per team)

UNIT VIII (C) OUTLINE

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, Units IX, Site and Layout Design Guidance, and X, Building Design Guidance are excellent opportunities to illustrate the concepts in this instruction unit as applied to the Local Area.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will answer questions in the Student Activity exercises using the Case Study to identify prevalent CBR threats (Design Basis Threat and others) and using FEMA 426 to answer selected filtration and mitigation measure questions.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page (Unit #) in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- 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. Display the charts applicable to the respective question to illustrate the answer.

- 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.

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

(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

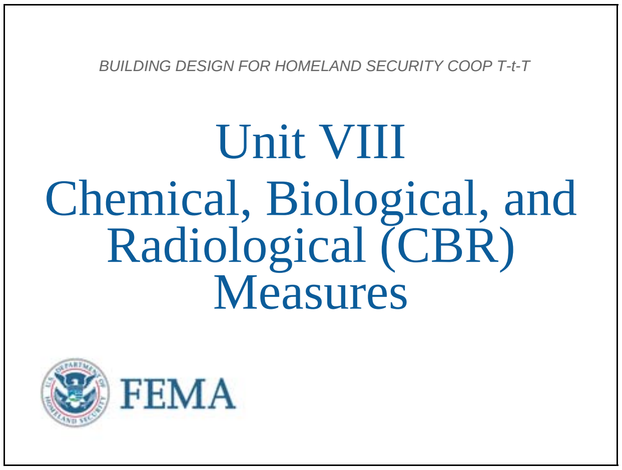
(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-1

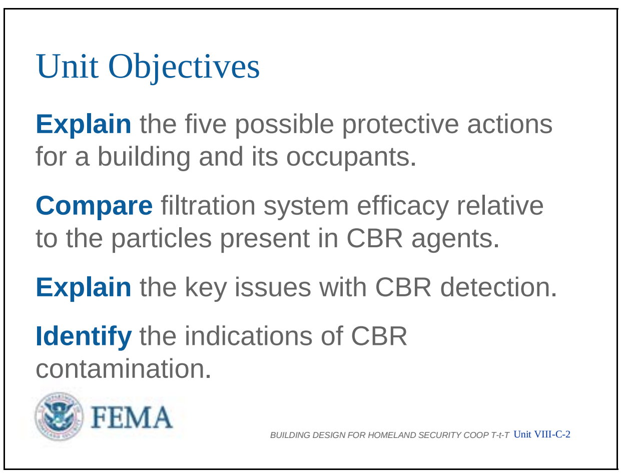


Introduction and Unit Overview

This is Unit VIII CBR Measures. In this unit, CBR protective measures and actions to safeguard the occupants of a building from CBR threats are presented. The unit is based largely on CDC/NIOSH and DoD guidance.

NOTE to instructor: Do not dwell upon the technical nature of CBR up to Visual VIII-C-41. Go over this front end quickly. Then concentrate on the mitigation measures in C-41 and beyond. However, actual incidents could receive additional explanation to better understand the threat.

VISUAL VIII-C-2



Unit Objectives

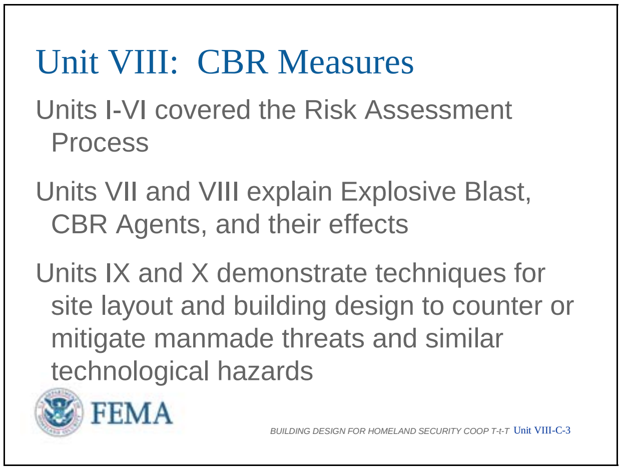
At the end of this unit, the students should be able to:

1. Explain the five possible protective actions for a building and its occupants.
2. Compare filtration system efficacy relative to the particles present in CBR agents.
3. Explain the key issues with CBR detection.
4. Identify the indications of CBR contamination.

NOTE to instructor: Emphasize that if your COOP facility's threats and hazards include CBR as nearby Hazardous Material or as Terrorist Attack, then this instruction unit provides what you need to know to make an initial assessment.

INSTRUCTOR NOTES

VISUAL VIII-C-3



CONTENT/ACTIVITY

CBR Measures

This unit is based on guidance from the CDC/NIOSH and the DoD and presents protective measures and actions to safeguard the occupants of a building from CBR threats. The following will be discussed:

- Evacuation
- Sheltering in place
- Personal protective equipment
- Air filtration and pressurization
- Exhausting and purging
- CBR detection

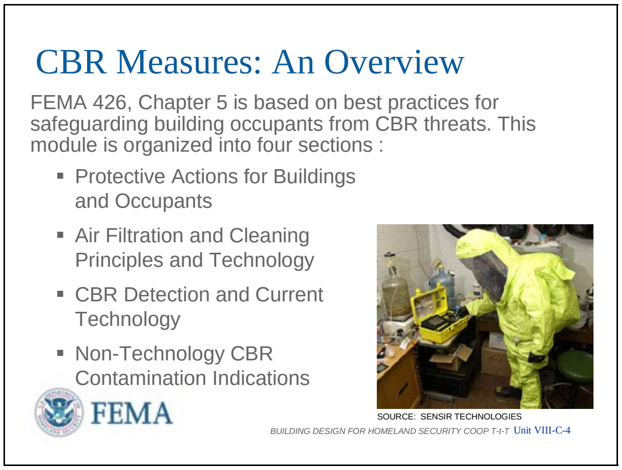
Additionally, CBR design and mitigation measures are discussed in:

- **Chapter 3 of FEMA 426**
- **Appendix C of FEMA 426** contains a glossary of CBR terms and a summary of CBR agent characteristics

Recent terrorist events have increased interest in the vulnerability of buildings to CBR threats. Of particular concern are building HVAC systems, because they can become an entry point and distribution system for airborne hazardous contaminants. Even without special protective systems, buildings can provide protection in varying degrees against airborne hazards that originate outdoors.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-4

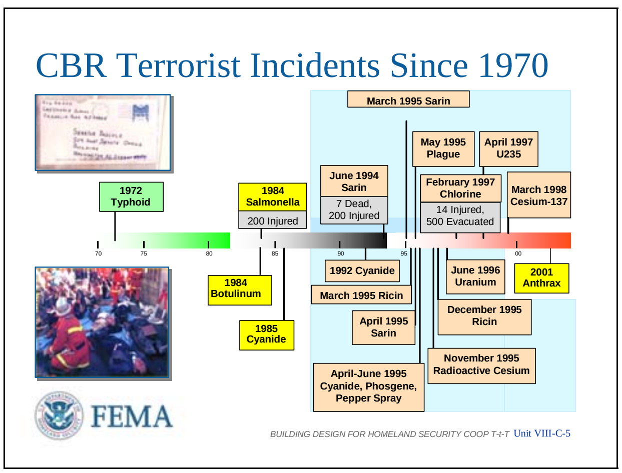


CBR Measures: FEMA 426 Chapter 5 Overview

This Unit draws on the latest research from CDC/NIOSH to present the best practices for detecting CBR agents, and safeguarding building occupants from the effects of CBR contamination.

Chapter 5 of FEMA 426 provides an overview on CBR Detection and Current Technology; and Indications of CBR Contamination, Evacuation, Sheltering in Place, Air Filtration and Pressurization, and Exhausting and Purging.

VISUAL VIII-C-5



CBR Terrorist Incidents Since 1970

CBR attacks have been used since ancient times and, in the past 20 years, over 50 attacks have occurred.

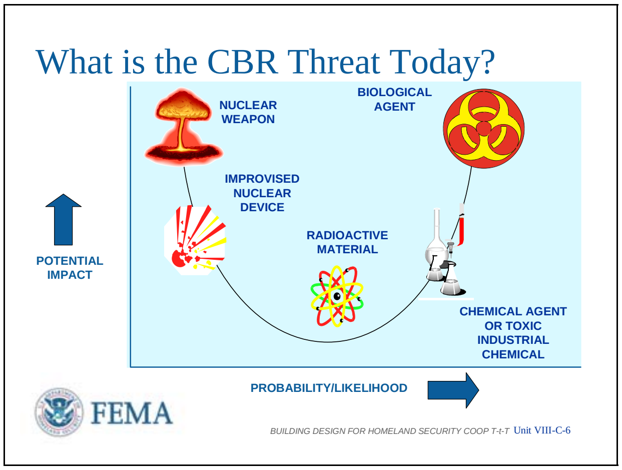
CBR attacks require the right weather, population, and dispersion to be effective.

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.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-6



What is the CBR Threat?

A fundamental question, *What is the CBR threat today?* This slide shows the relationship between the probability or likelihood of threats, and their potential impacts.

VISUAL VIII-C-7

Why Would Terrorists Use CBR?

- Available and relatively easy to manufacture
- Large amounts not needed in an enclosed space
- Easily spread over large areas
- Potential for mass casualties
  - Strong psychological impact
  - Overwhelms resources
  - Difficult to recognize (contagious or spread by victims

Recent events have shown that people not directly affected by the attack, but nearby, will seek medical confirmation of health / non-contamination and quickly overwhelm medical resources.

INSTRUCTOR NOTES

VISUAL VIII-C-8

VISUAL VIII-C-9

The slide shows the cover of Ben Laden's Terrorism Bible and The Mujahideen Poisons Handbook by Abdel Aziz. "Majahideen" - Arabic word meaning "holy warriors." This book is part of the Encyclopedia Jihad. The aim of this book is to further the military/ political preparations, skills and knowledge of Mujahideen the world over.

CONTENT/ACTIVITY

CBR Sources

There are many potential sources of chemical and biological agents, including laboratory and commercial production; and home production in those cases involving low concentrations of impure and inexpensive materials. Other sources include:

- Industrial facilities
- Foreign military sources
- Medical/university research facilities
- Nuclear facilities

The next series of slides will examine in more detail the properties of chemical and biological agents, **with implications for building design.**

Limitations of CBR Materials

- Targeted dissemination is difficult.
  While agents can be spread over a wide area with relative ease, targeting with sufficient concentration is much more difficult.
- Delayed effects can detract from impact.
  Terrorist seek immediate media impact, but many agents take time to result in impact
- Counterproductive to terrorists' support.
  Indiscriminate use of any WMD (Weapon of Mass Destruction), especially ones difficult to target with success, can attack innocents and those in the support base, thus reducing support of the populace for the terrorists' objectives.
- Potentially hazardous to the terrorist.
  Lack of expertise among terrorists can result in deadly contact with the CBR agents being produced, or premature

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

explosion of bombs during the bomb making process with deadly consequences

- Development and use require skill. More than one terrorist has produced bombs that will not explode and CBR agents that will not impact upon human beings to the level desired.

VISUAL VIII-C-10

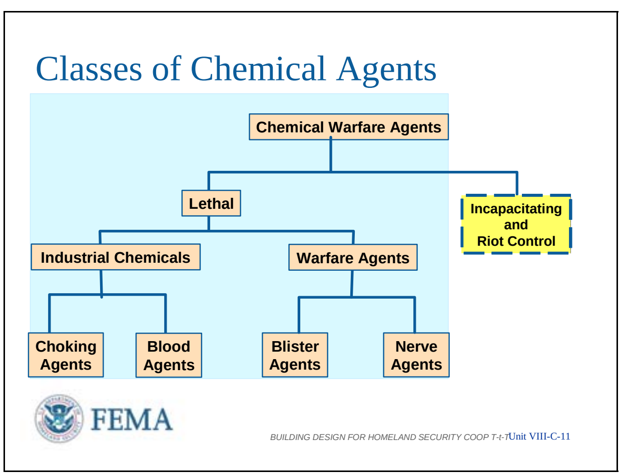
Subway riders injured in Aum Shinrikyo Sarin gas attack, in Tokyo, March 20, 1995.

Chemical Agents: Characteristics and Behavior

These are the general characteristics of chemical agents

- Liquids that are spread as aerosols or gases
- Impact breathing and attack exposed skin
- May have a distinct odor that allow detection
- Greatly influenced by the weather – rain, wind, sunlight, including its own physical characteristics – heavier or lighter than air

VISUAL VIII-C-11



Classes of Chemical Agents

Chemical agents are classified as either lethal or incapacitating and “riot control,” according to their intended use. For the purposes of this presentation, the emphasis has been placed on lethal agents as a consequence of their greater capacity for terrorist mischief.

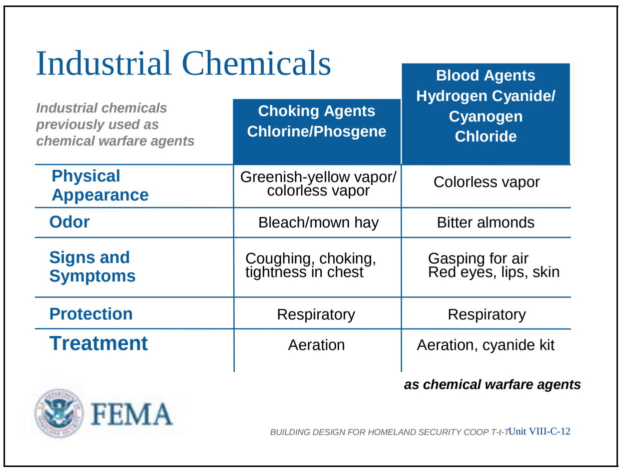
- **Lethal:** These have been subdivided into two categories: industrial materials used or considered as chemical warfare agents, and chemical warfare agents, which have little or no other purpose beyond their intended use as weapons of mass

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

destruction on the battlefield.

- **Incapacitating and Riot Control**: Not considered as primary terrorist threats, due primarily to their relatively short duration of effects and minimal toxicity. Therefore, they are not discussed in detail in this unit.

VISUAL VIII-C-12



Industrial Chemicals

This chart lists four industrial chemicals that were <u>previously used as chemical warfare agents</u>. These chemicals are used in the:

- Sanitation industry
- Plastics industry
- Pesticide industry.

All of these agents are generally respiratory agents and can be protected against by effective respiratory protection (i.e., self-contained breathing apparatus (SCBA)).

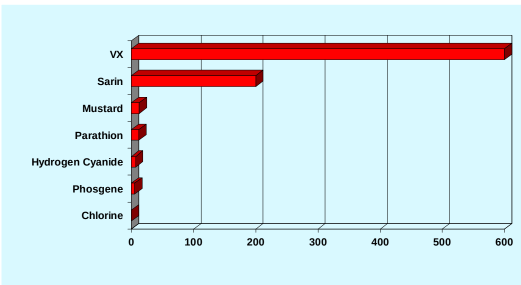
Skin contact with concentrated material may cause chemical burns and contact with eyes has similar effects as indicated by the MSDS (Material Safety Data Sheets) for these chemicals. However the main tactic for use of these chemicals does not seek this effect.

<u>They are all exceedingly volatile and dissipate rapidly outdoors</u>.

INSTRUCTOR NOTES

VISUAL VIII-C-13

Comparative Toxicity



FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-13

Note: At this point, reinforce the following: *…as we collectively examine and identify opportunities to improve building safety from CBR, it is important to understand the characteristics of CBR, and their potential consequences for the public, and first responders…. detailed information on the properties of these agents can be found in* ***Appendix C of FEMA 426****.*

VISUAL VIII-C-14

How Much Sarin Does it Take?

Structure	Lethal Amount
Domed Stadium	107 kg (26 gals)
Movie Theater	1.2 kg (5 cups)
Auditorium	52 g (1/4 cup)
Conference Room (50-100 seating)	33 g (1 shot glass)

LD_{50} amounts for 1 minute exposure to Sarin aerosol

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-14

CONTENT/ACTIVITY

Comparative Toxicity

This is a graphical comparison of the approximate lethalities of some chemical agents. They are based relative to Chlorine (CL or Cl) in terms of respiratory toxicity. If we use Chlorine as a baseline (1.0 on the graph):

- Phosgene (CG) is about 6 times more toxic.
- Hydrogen Cyanide (AC) is about 7 times more toxic.
- Parathion, an insecticide ingredient, is about 12 times more toxic.
- Mustard (H) is about 13 times more toxic.
- Sarin (GB) is about 200 times more toxic.
- VX (nerve agent) is about 600 times more toxic.

For skin toxicity, less than a pinhead of mustard agent is required to achieve a small blister. Less than a pinhead of VX can be lethal.

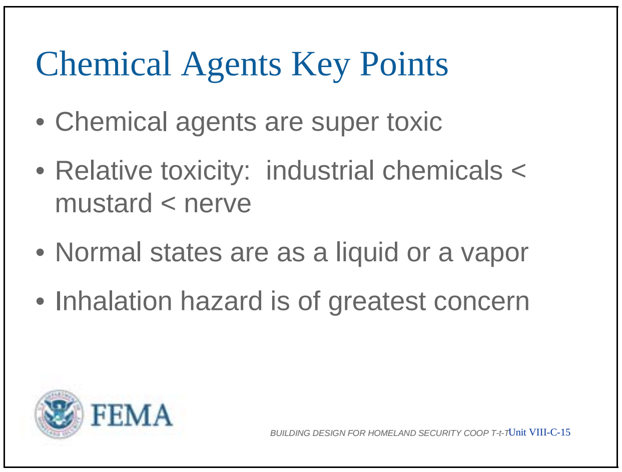
How Much Sarin Does it Take?

We have all heard of Sarin, which is among the most lethal of chemical agents. It is both odorless and colorless in pure form.

These numbers are the Lethal Doses 50 (LD_{50}) amounts for 1 minute of exposure to Sarin aerosolized liquid. This means that, in a 1-minute period, it would take approximately 26 gallons of Sarin to kill 50 percent of the people in a domed stadium, 5 cups of Sarin to kill 50 percent of the people in a movie theater, only about ¼ cup of Sarin to kill 50 percent of the people in an auditorium, and the equivalent of a shot glass to kill 50 percent of the people in a 50-100 person conference room.

It is the aerosol that is most often fatal. For example, the Tokyo subway attack used Sarin liquid and the liquid caused very few deaths. Most casualties were from the closed subway environment where the Sarin aerosolized (evaporated) on its own in the confined space of the subway reaching toxic levels.

VISUAL VIII-C-15

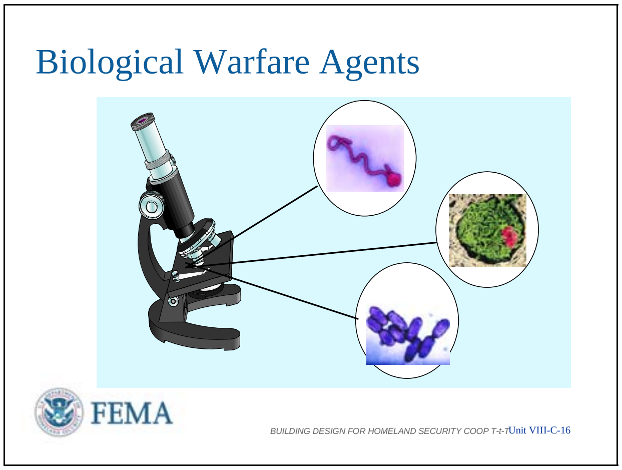


Chemical Agents Key Points

- Chemical agents are supertoxic. These agents were deliberately developed to cause injury or death to individuals.
- Relative toxicity: industrial chemicals < mustard < nerve. In terms of relative toxicity, the same amount of an industrial chemical is less toxic than a blister agent, and both are less toxic than a nerve agent.
- Normal states are as a liquid or a vapor. These agents are either a liquid or a vapor in their normal state. But the vapor is a more effective WMD.
- Inhalation hazard is of greatest concern. Nerve and blister agents pose both a skin and inhalation hazard. The inhalation hazard is of greater concern.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-16

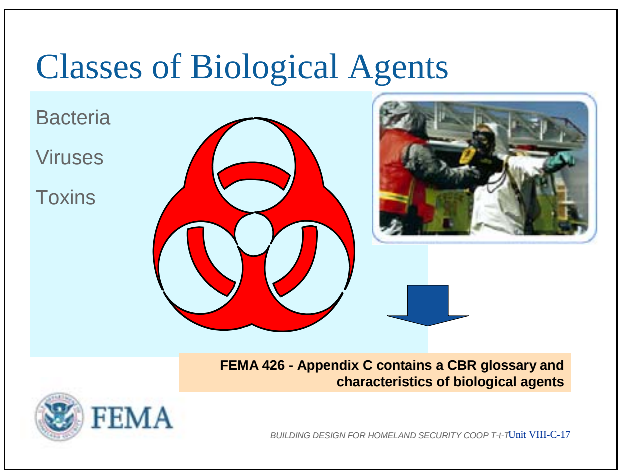


Biological Warfare Agents

Emphasize differences between chemical and biological agents:

- **Delayed effects:** The biggest difference is time. Unlike chemical agents, most of which have an immediate effect, most biological agents have a delayed effect ranging from several hours to days, and in some cases, weeks. In the event of a biological incident, there may be no casualties and nothing significant initially.
- **Toxicity:** By weight, biological agents are generally more toxic than chemical agents. For example, Ricin is 6 to 9 times more toxic than Sarin, and Botulinum, another toxin, is 15,000 to 30,000 times more toxic than Sarin.
- **Human detection:** Biological agents are undetectable by the human senses.

VISUAL VIII-C-17



Note: As we look at biological agents, you will see some similarities with what we discussed earlier with chemical agents, but you will also note some significant differences. Selected bacterial, viral, and toxin agents, their characteristics, and treatment are of particular concern when preparing

Classes of Biological Agents

- Both **bacteria** and **viruses** are living organisms and, as such, require an environment in which to live and reproduce.
- They can enter the body through inhalation or ingestion, through a break in the skin, or through other body openings or orifices.
- Once the organisms invade the body, they begin to grow and reproduce. They can also produce toxins that may poison the body.
- **Toxins** are poisonous substances produced as a byproduct of pathogens or plants and even some animals.

for biological terrorism.

VISUAL VIII-C-18

Bacteria

	Anthrax	Plague
Incubation Period	1 to 6 days	2 to 3 days for pneumonic 2 to 10 days for bubonic
Contagious	NO	YES (pneumonic) NO (bubonic)
Signs and Symptoms	Chills, fever, nausea, swollen lymph nodes	Chills, high fever, headache, spitting up blood, shortness of breath
Protection	Standard Precautions	Standard Precautions and Droplet Precautions
Treatment	Antibiotics and vaccines	Antibiotics and vaccines

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-18

VISUAL VIII-C-19

Viruses

	Smallpox	Viral Hemorrhagic Fevers
Contagious	YES	YES
Signs and Symptoms	Fever, rigors, vomiting, headache, pustules	Fever, vomiting, diarrhea, mottled/blotchy skin
Protection	Standard Precautions + Droplet + Airborne + Contact Precautions	Standard Precautions + Droplet + Airborne + Contact Precautions
Treatment	Vaccine, supportive therapy	Vaccines available for some

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-19

Bacteria

Anthrax and plague are two examples of diseases caused by bacteria. This chart highlights the important characteristics of each, including:

- Incubation period
- Whether they are contagious or not
- Signs and symptoms
- Protection
- Treatment

Again, a basic understanding of these characteristics will be valuable in developing an **appropriate and effective protective action strategy for your facility**.

Viruses

Two viruses are highlighted: **Smallpox** and **Viral Hemorrhagic Fevers**. Both are contagious, and protective actions include the use of standard, airborne, and contact precautions.

For example, most contagion in smallpox is from people inhaling small droplets from the coughing of infected/contagious persons.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-20

Toxins

	Neurotoxin (Botulinum)	Cytotoxin (Ricin)
Onset of Symptoms	1 to 3 days	4-8 hours after ingestion 12-24 hours after inhalation
Contagious	NO	NO
Signs and Symptoms	Weakness, dizziness, dry mouth and throat, blurred vision, paralysis	Chills, high fever, headache, spitting up blood, shortness of breath
Protection	Standard Precautions	Standard Precautions
Treatment	Supportive care, antitoxins, and vaccines	Supportive oxygenation and hydration

Note: There are numerous naturally-occurring toxins. For our purposes, we will group them into two categories.

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-20

Toxins

Finally, there are numerous naturally-occurring **toxins.** For our purposes, we will group them into two categories:

- **Neurotoxins:** Neurotoxins attack the nervous system. They are fairly fast-acting and can act in a manner opposite to that of the nerve agents because they prevent nerve-to-muscle stimulation.
- **Cytotoxins:** Cytotoxins are cell poisons. They are slower acting and can have a variety of symptoms, including vomiting, diarrhea, rashes, blisters, jaundice, bleeding, or general tissue deterioration.

There are numerous other modes of action of toxins, which are beyond our need to discuss here.

VISUAL VIII-C-21

Biological Agents Key Points

Onset of symptoms

Potentially contagious

Signs and symptoms

Protection

Treatment

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-21

Biological weapons are considered the emerging mass weapon of destruction of choice for terrorists because many agents can be made with standard commercial laboratory or brewing equipment.

Biological Agents Key Points

<u>NOTE: A very low dose of a biological agent can cause infection and spread disease, thus detection requires high sensitivity, but because there are many biologicals in the environment, detection requires selectivity, and since biological agents are very complex molecules making them difficult to identify/detect.</u>

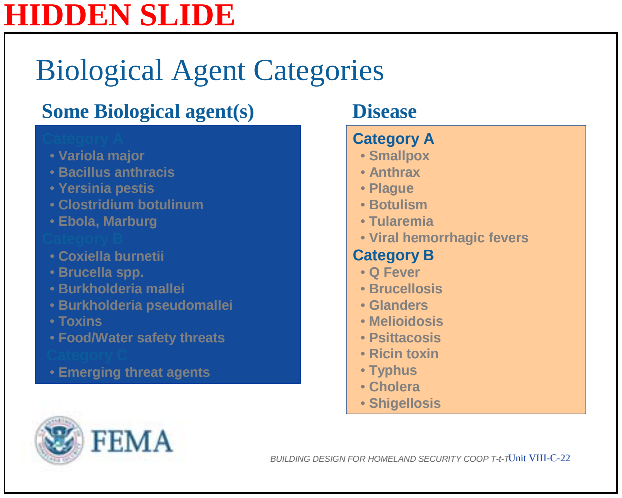
- **Onset of symptoms:** Most biological agents have an incubation period. Delayed effects will make identifying a biological attack more difficult.
- **Potentially Contagious**: <u>Only a few</u> biological agents are <u>contagious</u>: plague, smallpox, and viral hemorrhagic fevers (VHF), such as Ebola.
- **Signs and symptoms**: Signs and symptoms of many biological attacks initially manifest themselves as flu-like; therefore, it may be difficult to identify that an attack has occurred.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

- **Protection:** Standard precautions will be adequate protection against most biological agents.
- **Treatment:** Some biological agents can be treated with antibiotics, vaccines, and antitoxins; for agents for which there are none of the aforementioned treatments, supportive care should be administered, such as treating the symptoms.

The recent SARS and Avian Flu outbreaks demonstrate the relative ease by which naturally-occurring biological agents can quickly transmutate and spread across the globe. The flu strain that caused the Flu Pandemic of 1918 is still an active strain.

VISUAL VIII-C-22
HIDDEN SLIDE



Biological Agent Categories

Agents are placed in one of three priority categories for initial public health Preparedness efforts based on the overall criteria and weighting of each agent.

Category A: Carry the highest priority because they:

- Can be easily disseminated or spread person-to-person
- Can be highly lethal
- Have the potential for serious public health impact
- Can potentially cause public panic and lead to social disruption

Category B: Carry the second-highest priority because they:

- Are moderately easy to disseminate
- Usually result in moderate morbidity
- Are generally less lethal

Category C: They include emerging pathogens that could potentially be engineered for future mass dissemination.

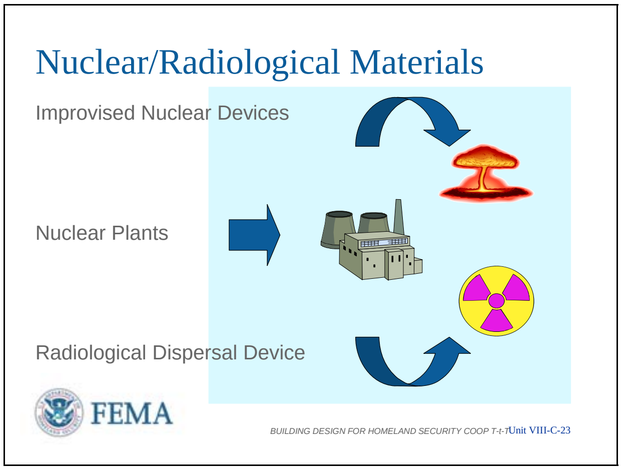
- Nipah virus

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Hantavirus

Not believed to present a high bio terrorism risk to the public health today, but could emerge as future threats.

VISUAL VIII-C-23



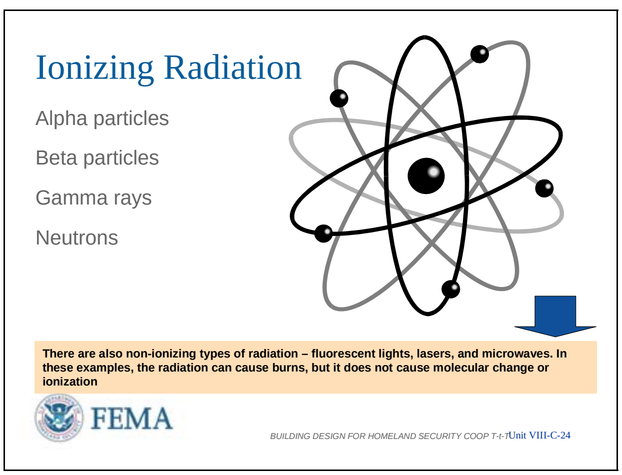
Nuclear/Radiological Materials

Of the three types of threats (chemical, biological, or nuclear/radiological), a **nuclear weapon explosion** is considered the least likely for terrorist use; however, the potential exists for it to happen and even more potential exists for the use of radiological materials.

Possible scenarios:

- Detonation of an **improvised nuclear device** (IND)
- Terrorist attack on a **nuclear plant**
- Use of a **radiological dispersal device** (RDD), or "dirty" bomb – the simple act of spreading the materials

VISUAL VIII-C-24



Note: In its simplest definition, radiation can be defined as either electromagnetic or particulate emissions of energy from the disintegration of the nucleus of an atom. This energy, when impacting on or passing through material,

Ionizing Radiation

Ionizing radiation is either particle radiation or electromagnetic radiation in which an individual particle/photon carries enough energy to ionize an atom or molecule by completely removing an electron from its orbit. If the individual particles do not carry this amount of energy, it is essentially impossible for even a large flood of particles to cause ionization. These ionizations, if enough occur, can be very destructive to living tissue, and can cause DNA damage and mutations.

For our purposes, ionizing radiation includes:

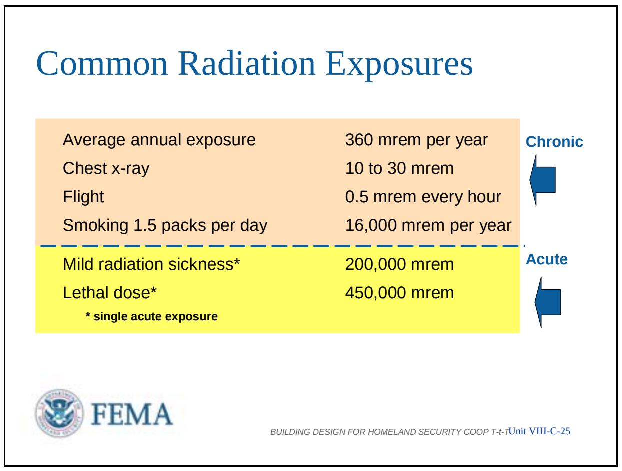
- **Alpha particles**
- **Beta particles**
- **Gamma rays**
- **Neutrons**

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

including humans, can cause some form of reaction.

Radioactive material: Any material that is giving off some form of ionizing radiation.

VISUAL VIII-C-25



Note: Mild radiation sickness (i.e., nausea, vomiting, and diarrhea) may onset after receiving a whole body dose of approximately 200,000 mrem in a short amount of time (generally less than 24 hours). The Lethal Dose (LD), known as the LD50/60, is a single, acute, whole body exposure of around 450,000 mrem. The LD50/60 is defined when 50 percent of all people present at an incident receive 450,000 mrem and die after 60 days after receiving no medical treatment.

Dose in rem = RBE x dose in rad
RBE = 1 for gamma radiation and beta radiation above 30,000 electron volts
RBE = 0.7 for photons above 4 million electron volts (minimum found)

Again, for the purposes of this course, we are primarily concerned with the *hazard*, the *detection* of the hazard, and *protective* actions that we can take.

Ionizing radiation is what causes injury or death, and is also a characteristic by which nuclear materials can be measured and identified.

Common Radiation Exposures

This chart reflects naturally-occurring radiation doses (and doses received during normal activities) to provide a point of reference and for comparison. The threshold for any real consequences begins around 200,000 mrem.

The average annual radiation exposure has been calculated as:

Naturally occurring	295 mrem
Medical	52 mrem
Consumer products	10 mrem
Other	3 mrem
Total	*360 mrem*

mrem = millirem
milli- = 10^{-3} or "one thousandth of"
rem = **röntgen** (**roentgen**) **equivalent** in **man** Pronounced "rho – ent – gen" with a long "o" and the two "e" are short
rem is a unit of equivalent dose, much like TNT equivalent for explosives. Rem relates the absorbed dose in human tissue to the effective biological damage of the radiation. Not all radiation has the same biological effect, even for the same amount of absorbed dose.
rad is the unit of absorbed dose equal to 100 ergs per gram or 0.01 joule per kg.

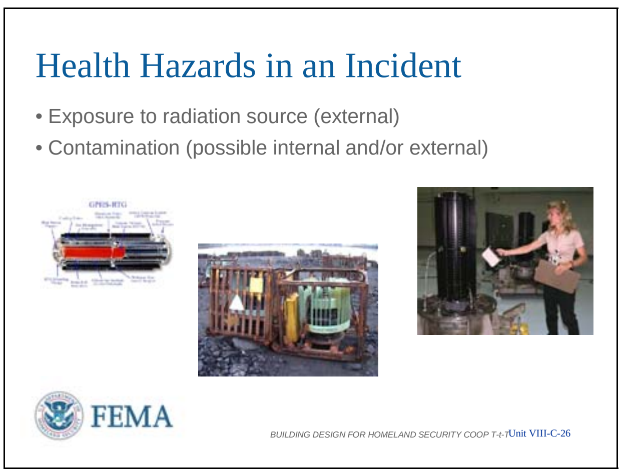
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

RBE = 20 for heavy ions (maximum found)

(Energy and mass, but not biological damage)

Source of radioactivity in smoking is Lead 210 (beta radiation) and Polonium 210 (alpha radiation) which comes as Radon 222 gas from the soil and is absorbed by the tobacco plant’s leaves. While the tobacco plant takes up little radioactivity from the soil directly like it draws other nutrients, it turns out that “developed” countries usually fertilize their tobacco fields with chemically manufactured fertilizer high in phosphate content to make the tobacco more “flavorful” than if nitrogen based fertilizer is used as in poorer countries. The phosphate portion of this fertilizer is made from a rock mineral, apatite, which is ground to powder, dissolved in acid and further processed. Apatite rock contains Radium 226 (the precursor of Radon 222).

VISUAL VIII-C-26



Note**:** Internal exposure through wounds or broken skin is also possible. Responders should take extra precautions when sharp objects, such as broken glass or jagged metal, are at the scene.

Left Photo - This image shows the cut-away of an actual Radioisotope Thermoelectric Generators (RTG) Unit which produces

Health Hazards

The two radiation concerns at an incident are exposure and contamination by radioactive material. External irradiation occurs when all or part of the body is exposed to penetrating radiation from an external source. Contamination means that radioactive materials in the form of gases, liquids, or solids are released into the environment and get on people externally, get in them internally, or both.

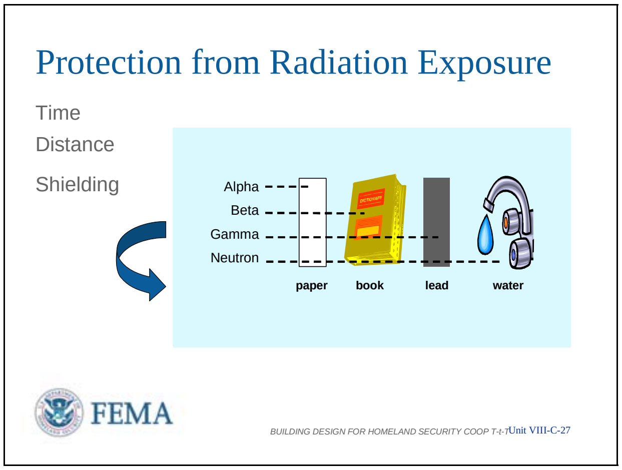
Incidents involving either an explosion or fire will elevate the potential for internal or external contamination due to the spreading of the radioactive material in the form of small fragments (dust) or smoke. These materials can often be carried long distances downwind.

Radiological materials are both colorless and odorless.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

electricity via the thermoelectric effect.
Center Photo - RTG from the Cassini program.
Right Photo - RTG abandoned on the Kola Peninsula, Russia

VISUAL VIII-C-27



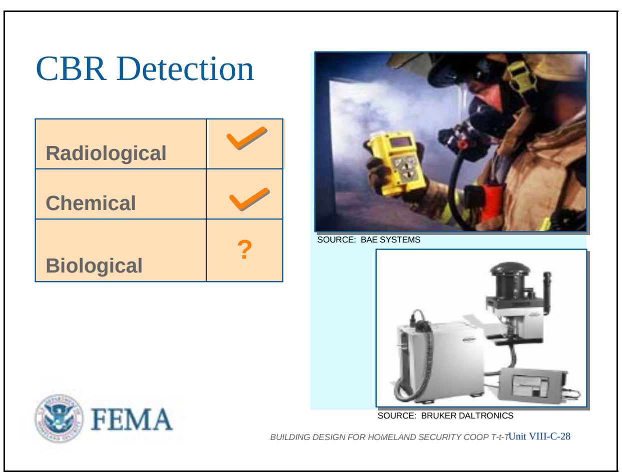
Note: Do not shield neutron-producing sources with lead or dense materials as the neutrons react with the material to produce gamma rays. Use wax, water, or plastic instead.

Protection from Radiation Exposure

The radiation exposure received will depend on the type and strength of radiation source. This exposure can be reduced by effective use of:

- **Time:** The radiation dose is reduced in proportion to reduction in exposure time.
- **Distance:** Distance is also critical for reducing radiation exposure dose. Although alpha particles only travel a little over an inch in air, and beta particles will travel only a few yards in air, gamma rays can travel extensive distances.
- **Shielding:** Radiation can also be blocked or reduced by various materials. Alpha radiation is stopped by a sheet of paper, beta radiation is stopped by aluminum foil or clothing, gamma rays are only reduced by dense materials such as lead or earth, and neutrons are slowed or stopped by hydrogenous materials, such as wax or water.

VISUAL VIII-C-28



CBR Detection

The underlying theme of this chapter is that effective protection against potential releases of CBR is a function of:

1) Effective and timely detection of the agent(s); and
2) A public that is knowledgeable of the most appropriate protective actions to take in the event of a CBR release.

The discussion on **CBR detection** includes:

- CBR detection technology currently available.

INSTRUCTOR NOTES

Sources of useful technical information:

- *NBC Products and Services Handbook* contains a catalogue of CBR detection equipment.
- *Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders*, published by the National Institute of Justice (NIJ) (Guide 100-00, Vols 1 & 2), June 2000.
- *An Introduction to Biological Agent Detection Equipment for Emergency First Responders*, published by the NIJ (Guide 101-00): December 2001.

CONTENT/ACTIVITY

- Indications of CBR contamination.
- <u>Mass spectrometry. (can positively identify a chemical agent at very low concentrations)</u>
- Most strategies for protecting people from airborne hazards require a means of detection (determining that a hazard exists).
- **Chemical detection** technology has improved vastly since Operation Desert Storm (when many military detection systems experienced high false-alarm rates). Current chemical detectors work in about 10 seconds.
- **Biological detection** technology has not matured as fast; generally require trained specialists to administer; biological signatures can take 30 minutes to detect. <u>Biological detection requires sensitivity (very low effective dose must be detected), selectivity (there are many biologicals in the environment, thus must discern the contagious/deadly ones), and identification of very complex molecules (the complexity makes them difficult to identify).</u>

A variety of **radiological detectors** have been developed for the nuclear industry and are commercially available.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-29

CBR Incident Indicators

Indicator	Chemical	Biological	Radiological
Dead Animals	✔		✔
Lack of Insect life	✔		
Physical Symptoms	✔	✔	✔
Mass Casualties	✔		✔
Unusual Liquids	✔		
Unexplained Odors	✔		
Unusual Metal Debris/Canisters	✔	✔	✔
Heat Emitting or Glowing			✔
Spray Mechanisms	✔	✔	

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-TUnit VIII-C-29

In general, chemical agents will typically have a rapid onset of symptoms, while the response to biological or radiological agents can be delayed. Potential indicators of threats include suspicious packages or containers or unusual powders or liquids, droplets, mists, or clouds found near air-intake, in air-ventilation ductwork, and HVAC systems.

CBR Incident Indicators

This is a summary table indicating warning properties of CBR agents in terms of dead animals, lack of insect life, physical symptoms, mass casualties, unusual liquids, unexplained odors, unusual metal debris, heat emitting or glowing, and <u>spray mechanisms.</u>

Details provided in visuals VIII-C-30, -31, -32, and -33.

VISUAL VIII-C-30
HIDDEN SLIDE

Chemical Incident Indicators (1)

Dead animals, birds, fish	Not just an occasional roadkill, but numerous animals (wild and domestic, small and large), birds, and fish in the same area.
Lack of insect life	If normal insect activity (ground, air, and/or water) is missing, check the ground/water surface/shore line for dead insects. If near water, check for dead fish/aquatic birds.
Physical symptoms	Numerous individuals experiencing unexplained water-like blisters, wheals (like bee stings), pinpointed pupils, choking, respiratory ailments, and/or rashes.
Mass casualties	Numerous individuals exhibiting unexplained serious health problems ranging from nausea to disorientation to difficulty in breathing to convulsions to death.
Definite pattern of casualties	Casualties distributed in a pattern that may be associated with possible agent dissemination methods.

Chemical agents have a rapid onset of symptoms

FEMA

FEMA 426, Table 5-2: Indicators of a Possible Chemical Incident, p. 5-34

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-TUnit VIII-C-30

Chemical Incident Indicators (1)

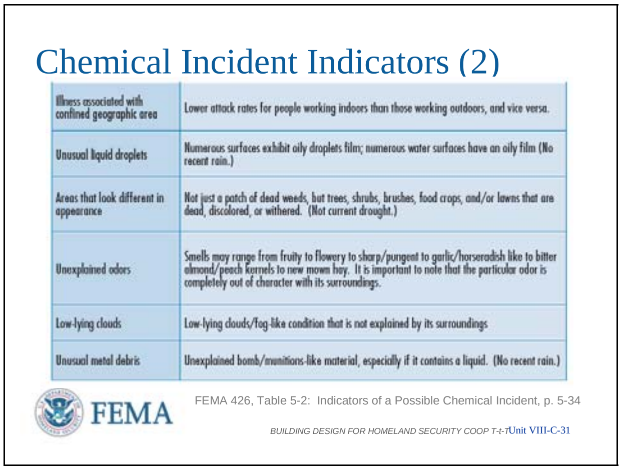
Most hazardous chemicals have warning properties that provide a practical means for detecting a hazard and initiating protective actions. Such warning properties make chemicals perceptible; for example, vapors or gases can be perceived by the human senses (i.e., smell, sight, taste, or irritation of the eyes, skin, or respiratory tract) before serious effects occur.

In the absence of a warning property, people can be alerted to some airborne hazards by observing symptoms or effects in others. This provides a practical means for initiating protective actions, because the susceptibility to hazardous materials varies from person to person.

INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL VIII-C-31
HIDDEN SLIDE

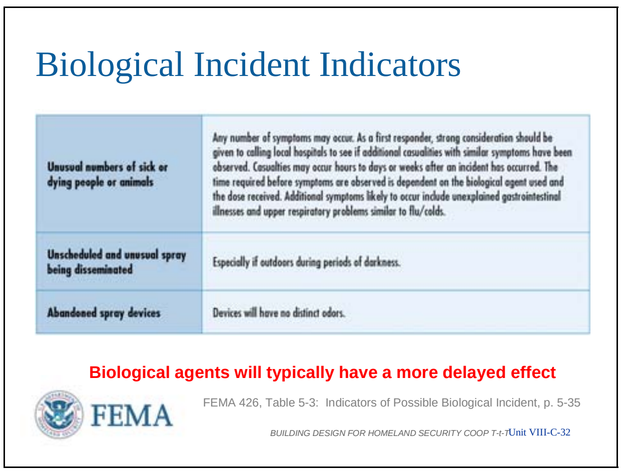


Chemical Incident Indicators (2)

Chart 2 depicts the following chemical indicators:

- Definite pattern of casualties
- Illness associated with a confined geographic area
- Unusual liquid droplets
- Areas that look different in appearance
- Unexplained odors
- Low-flying clouds
- Unusual metal debris

VISUAL VIII-C-32
HIDDEN SLIDE



Biological Incident Indicators

In the case of a biological incident, the onset of symptoms takes days to weeks and, typically, there will be no characteristic indicators. Because of the delayed onset of symptoms in a biological incident, the area affected may be greater due to the migration of infected individuals.

<u>The indicators of biological attack easiest to identify are unscheduled and unusual spraying and abandoned spray devices.</u>

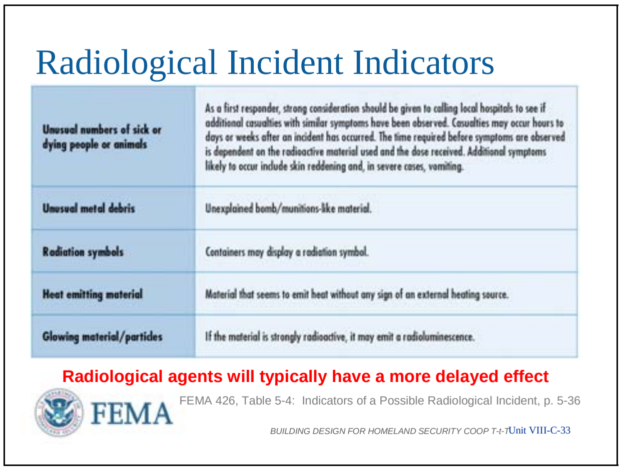
Let's make a distinction between bioterrorism against people and against animals:

> **People**: Farmers might see cows/livestock get anthrax after an anthrax biological attack (but not cats and dogs). No other commonly discussed biological agents used for people will affect animals. Alternately, rats carry fleas that spread plague, but the rats don't get plague.
>
> **Animals**: Unlikely to happen and if it does few people are going to see it for what it is. It makes another distinction between biological and chemical

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

indicators. However, if the attack is against animals, then animal effects are indications. For example foot and mouth disease or pseudo rabies or swine flu or bird flu would cause huge animal loses but no human deaths (unless you count the recent bird flu deaths by people handling infected poultry and this in contact). But these latter instances are not bioterrorism yet.

VISUAL VIII-C-33
HIDDEN SLIDE

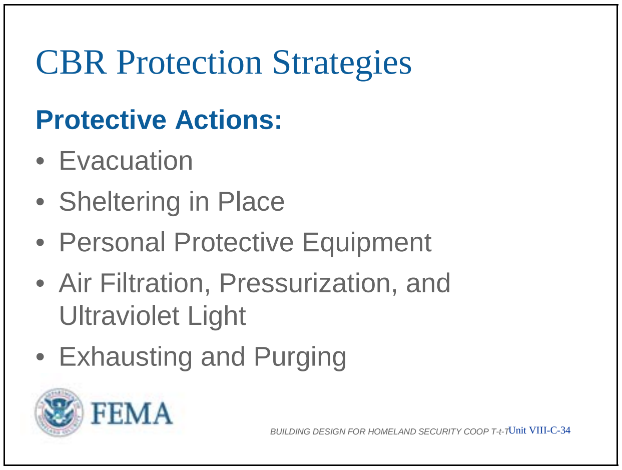


Radiological Incident Indicators

In the case of a radiological incident, the onset of symptoms also takes days to weeks to occur and typically there will be no characteristic indicators. Radiological materials are not recognizable by the senses because they are colorless and odorless.

It is fortunate the radiological detectors are so mature to detect radiation sources and residual radiation.

VISUAL VIII-C-34



CBR Protection Strategies

Once the presence of an airborne hazard is detected, there are five possible **protective actions** for a building and its occupants. In increasing order of complexity and cost, these actions are:

- Evacuation
- Sheltering in Place
- Personal Protective Equipment
- Air Filtration and Pressurization
- Exhausting and Purging

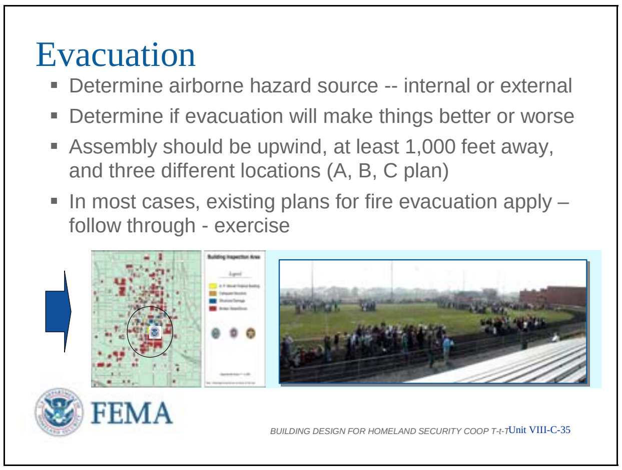
To ensure the protective actions are effective you must have:

INSTRUCTOR NOTES	CONTENT/ACTIVITY

- A protective action plan specific to each building
- Training and familiarization for occupants

Protective actions are discussed in more detail in the following sections.

VISUAL VIII-C-35



This map displays 1,000 foot radius to determine minimum evacuation distance, 2,000 feet would be better.

Evacuation

- Evacuation is the most common protective action taken when an airborne hazard, such as smoke or an unusual odor, is perceived in a building.
- There must be some detection method or knowledgeable personnel in place to make the determination of what to do – evacuate or some other action. This may be trained first responders, but even their response time can be too long depending upon the situation.
- Orderly evacuation is the simplest and most reliable action for an internal airborne hazard, but may not be the best action in all situations, especially in the case of an external CBR release, particularly one that is widespread.
- If some agent has infiltrated the building and evacuation is deemed not to be safe, the use of protective hoods may be appropriate.
- The evacuation plan should list each contingency and the decision process.

VISUAL VIII-C-36

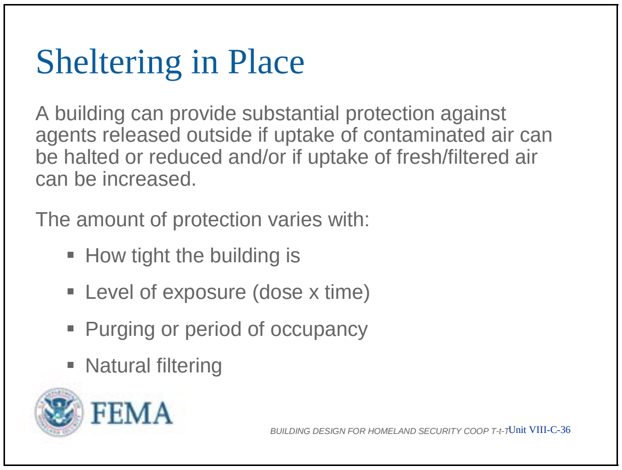
Sheltering in Place

Interrupting the flow of fresh air is the principal applied in the protective action known as sheltering in place.

Advantage: It can be implemented rapidly.

Disadvantage: Protection is variable and

INSTRUCTOR NOTES



In most cases, air conditioners and combustion heaters cannot be operated while sheltering in place because operating them increases the outdoor-indoor exchange of air.

Sheltering in place is, therefore, suitable *only for exposures of short duration,* roughly 2 hours or less, depending on conditions.

Because the building slowly releases contaminants that have entered, at some point during cloud passage the concentration inside exceeds the concentration outside. Maximum protection is attained by increasing the air exchange rate after cloud passage or by exiting the building into clean air. The tighter the building, the greater the effect of this natural filtering.

FEMA 453 covers square footage required per person for various short and long term situations for people of various capabilities.

CONTENT/ACTIVITY

diminishes with the duration of the hazard.

The level of protection that can be attained by sheltering in place is substantial, but it is less than can be provided by high-efficiency filtration of the fresh air introduced into the building.

The amount of protection varies with:

The building's air exchange rate. The tighter the building (i.e., the lower the air exchange rate), the greater the protection it provides.
- Sealing dampers on air intakes
- Previously sealed all identifiable air leakage in building envelope (smoke test or infrared survey on very hot or very cold day)
- This presupposes that all HVAC and other mechanical means that move air, including bathroom exhausts and elevators, are shutdown to not draw outside air into the building

The level of exposure. Protection varies with agent concentration and time, diminishing as the time of exposure increases or as concentration of agent increases. Thus a high-concentration plume passing quickly over a building would indicate sheltering in place to be the best option.

Purging or period of occupancy. How long occupants remain in the building after the hazardous cloud has passed also affects the level of protection. However, after the high-concentration plume passes, there will be some inleakage of agent that does occur and the longer one stays in the building the higher the exposure, unless the building is purged or aired out.

Natural filtering. Some filtering occurs when the agent is deposited in the building shell or upon interior surfaces as air passes into and out of the building.

INSTRUCTOR NOTES

VISUAL VIII-C-37
HIDDEN SLIDE

Note: Although sheltering is for protection against an external release, it is possible, but more complex, to shelter in place in one or more floors of a multi-story building after an internal release has occurred. In these circumstances, it is critical to turn off all air handling equipment, isolate stairwells, and not use elevators.

CONTENT/ACTIVITY

Sheltering in Place

If the office environment is complex, planning and exercises are important. The sheltering plan should include:

- Identifying all air handling units, fans, bathroom exhausts, and the switches needed to deactivate them
- Identifying cracks, seams, and joints in the building shell to be permanently sealed or temporarily sealed, along with sealing doors with duct tape
- Prepositioning supplies that are needed to initiate and sustain sheltering in place
- Identifying safe rooms or safe havens
- Identifying procedures for purging or airing out after an internal release
  - This must be done on a case-by-case basis for the agent involved and the agent concentration to be spread during the purging.
  - Competent first responder authority may best make this determination.
  - Sealing the release area and evacuating the building may be a better option and do not touch those purge fans!
- Identifying procedures for voluntary occupant participation
  - <u>During an event, the decision to shelter in place is voluntary</u>
  - Current law does not require people to use the shelter
  - People should enter the designated shelter area within 3-5 minutes. Depending upon plume speed and distance to travel, even this may be too long.
- Maintaining communications to understand what is occurring by monitoring TV or radio

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-38

Note: This slide depicts individuals wearing universal-fit escape hoods (upper left-hand corner picture and middle picture on the slide) that have been developed for short-duration "escape-only" wear to protect against chemical agents, aerosols (including biological agents), and some toxic industrial chemicals. The hoods are compact enough to be stored in desks (see picture in upper left-hand corner of the slide) or to be carried on the belt.

Personal Protective Equipment

- A wide range of **individual protection equipment** is available, including respirators, protective hoods, protective suits, CBR detectors, decontamination equipment, etc.
- If masks have been issued, ensure that training is conducted on how to put on and wear the masks.
- No selection of personal protective equipment is effective against every possible threat. Selection must be tied to specific threat/hazard characteristics.
- Universal hoods designed for short duration escape wear only protect against chemical agents by using both HEPA and carbon filters.
  - Carbon filters are designed to filter a broad range of toxic chemicals, but not all chemicals.
  - The EVAC-U8 hood was recalled in April 2006 due to a problem with removing carbon monoxide, which was a stated claim, applicable to its use as a fire escape hood, but it is NOT a CBR hood.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VIII-C-39

Shows pictures of aftermath of the tragic 9-11 events.

9-11 Dramatic Events

Assembly should be to the upwind side of the building and at least 1,000 feet away, since any airborne hazard escaping the building will be carried downwind.

<u>Starting from top left:</u>

Photo 1 - Remains Recovery

Photo 2 - Evacuation by Helicopter

Photo 3 - Arlington County EMS (Emergency Medical Services) unit

Photo 4 – NMRT (National Medical Response Team) decontamination corridor

<u>Bottom left:</u>

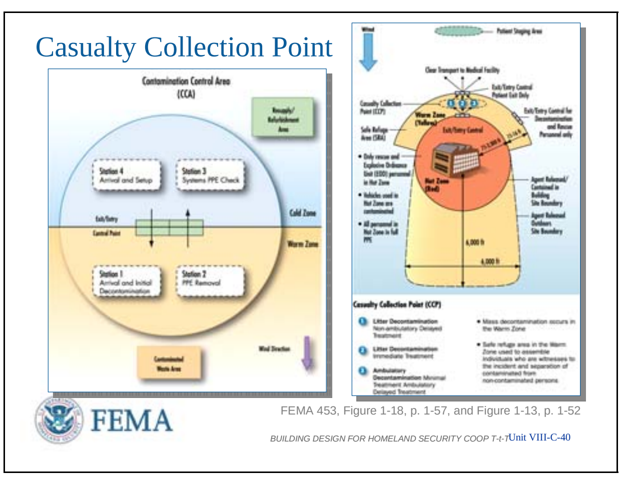
Photo 5 - Evidence Collector

Photo 6 - Man covered in debris from the Twin Towers collapse

Photo 7 - FEMA Urban Search and Rescue (US&R) Team from Montgomery County, MD is briefed before beginning work at Pentagon following 9-11 attacks.

Photo 8 - FBI and US&R

VISUAL VIII-C-40



Casualty Collection Point

Emergency operations need to be designed to allow law, fire, and medical vehicles and personnel access for mass decontamination operations.

The Contamination Control Area is located on the boundary of the Cold Zone and Warm Zone and used by the rescue and decontamination personnel to enter and exit the Warm Zone. There are several processing stations, a resupply and refurbishment area, and a contaminated waste storage area. Runoff from

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

<u>To summarize the right column:</u>
During planning, you need to identify the following on your site as part of your OEP (Occupant Emergency Plan):

- Areas for victims that require transportation
- Areas for rescue and decontamination personnel
- Areas for survivors that require decontamination

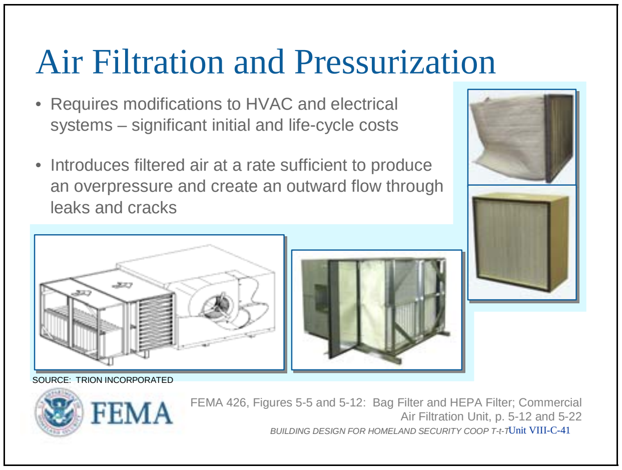
decontamination operations must be controlled or contained to prevent further site contamination.

Casualty Collection Point is a critical element to save lives. The following operations may take place during an emergency operation.

- The Patient Staging Area (PSA) is located in the Cold Zone and is the transfer point for victims that have been stabilized for transport to higher care medical facilities or for fatalities to be transported to morgue facilities. The PSA area must be large enough to accommodate helicopter operations and a large number of ambulances.
- The Casualty Collection Point is located in the Warm Zone and will have typically have three processing stations:
  - Station 1 – Litter decontamination and non-ambulatory delayed treatment patients
  - Station 2 – Litter decontamination and immediate treatment patients
  - Station 3 – Ambulatory decontamination, minimal treatment patients, and ambulatory delayed treatment patients
- Mass casualty decontamination occurs in the Warm Zone. The Safe Refuge Area is located in the Warm Zone and is used to assemble individuals who were witness to the incident and separation of contaminated from non-contaminated persons.

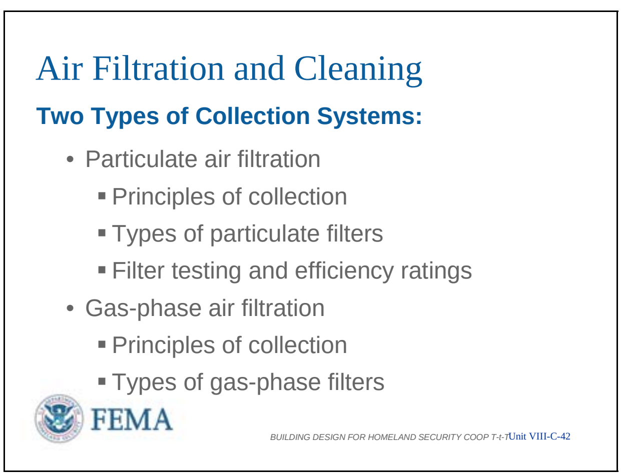
INSTRUCTOR NOTES

VISUAL VIII-C-41



Note: Applying external filtration to a building requires modification to the building's heating, ventilation, and air conditioning (HVAC) system and electrical system. These changes are necessary to ensure that, when the protective system is in operation, all outside air enters the building through filters. The air exchange that normally occurs due to wind pressure, chimney effect, and operation of fans must be reduced to zero.

VISUAL VIII-C-42



See CDC/NIOSH *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical,*

CONTENT/ACTIVITY

Air Filtration and Pressurization

- Two basic methods of applying air filtration to a building are external filtration and internal filtration. External filtration involves filtering and/or cleaning of the air drawn from the **outside,** while internal filtration involves filtering and/or cleaning of the air drawn from **inside** the building. Both methods require HVAC modifications that can be costly.

- Among the various protective measures for buildings, high efficiency air filtration/cleaning provides the highest level of protection against an outdoor release of hazardous materials.

NOTE to instructor: Emphasize to students that from this slide on the information will help the student to understand CBR issues and how to mitigate HVAC Systems when vulnerabilities are noted.

Air Filtration and Cleaning

Air filtration is the removal of particulate contaminants from the air. Air cleaning is the removal of gases or vapors from the air. The collection mechanisms for these two types of systems are very different.

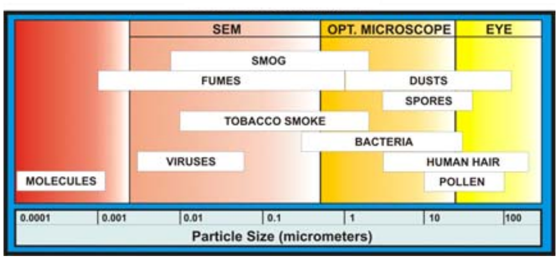
Particulate air filtration consists of fibrous materials, which capture aerosols. Their efficiency will depend on the size of the aerosol, the type of filter, the velocity of the air, and the type of microbe. The basic principle of particulate air filtration is not to restrict the passage of particles by the gap between fibers, but by altering the airflow streamlines. The airflow will slip around the fiber, but higher density aerosols and particulates will not change direction as

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Biological, or Radiological Attacks. Publication No. 2003-136, April 2003 for good explanations of these two types of filtration.

VISUAL VIII-C-43

Air Contaminant Sizes



FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-TUnit VIII-C-43

rapidly. Particulate filters are not intended to remove gases and vapors.

Gas-phase air filtration sorbent filters use one of two mechanisms for capturing and controlling gas-phase air contaminants: physical adsorption and chemisorption. Both mechanisms remove specific types of gas-phase contaminants in indoor air. Unlike particulate filters, sorbents cover a wide range of highly porous materials, ranging from simple clays and carbons to complex engineered polymers. Activated carbon is the most common sorbent, but does not capture all chemicals.

Sorbent filtration needs adequate residence time to ensure adsorption of the gas or vapors; that is adequate contact time for the flow rate of the air passing through the filters. In some cases, two sorbent filters may be needed in series to achieve needed residence time.

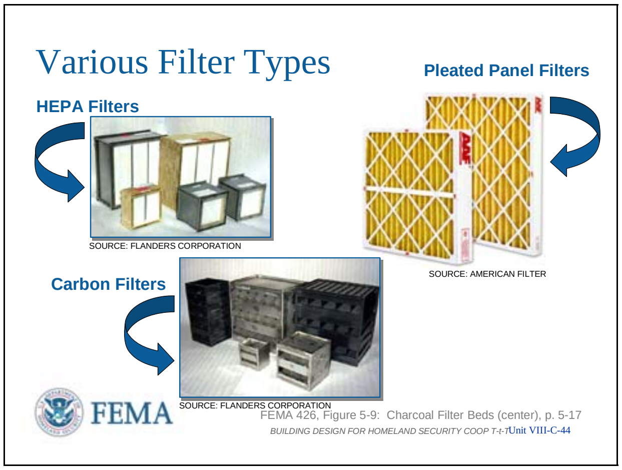
Air Contaminant Sizes

This chart illustrates the particle size for a number of the chemical, biological, and radiological agents of concern. Viruses are the smallest and most difficult to protect against.

In **FEMA 426, Table 5-1, page 5-12,** lists the new ASHRAE 52.2 Standards for particulate filter ratings to remove a given particle size. In most cases, new generation **Minimum Efficiency Reporting Value** (MERV) 11 to MERV 13 [**removal down to 0.3 to 1 micron**] filters can be used in commercial buildings and **effectively remove most particulates of CBR concern**.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-44



Various Filter Types

A wide variety of filters are available to meet many specialized needs:

HEPA (high efficiency particulate air) **Filters** - high performance filters that are typically rated as 99.97 percent effective in removing dust and particulate matter greater than 0.3 micron in size.

Carbon Filters - sorbent filters (gas-phase) that remove gas and vapors using the thousands of bonding sites on the huge surface area of activated carbon.

Pleated Panel Filters - particulate air filters consisting of fibrous materials that capture aerosols.

VISUAL VIII-C-45

ASHRAE Standards

ASHRAE 52.2				ASHRAE 52.1		Particle Size Range, µm	Applications
MERV	Particle Size Range			Test			
	3 to 10 µm	1 to 3 µm	.3 to 1 µm	Arrestance	Dust Spot		
1	< 20%	-	-	< 65%	< 20%	> 10	Residential, light, pollen, dust mites
2	< 20%	-	-	65 - 70%	< 20%		
3	< 20%	-	-	70 - 75%	< 20%		
4	< 20%	-	-	> 75%	< 20%		
5	20 - 35%	-	-	80 - 85%	< 20%	3.0 - 10	Industrial, Dust, Molds, Spores
6	35 - 50%	-	-	> 90%	< 20%		
7	50 - 70%	-	-	> 90%	20 - 25%		
8	> 70%	-	-	> 95%	25 - 30%		

FEMA

FEMA 426, Table 5-1: Comparison of ASHRAE Standards 52.1 and 52.2, p. 5-12

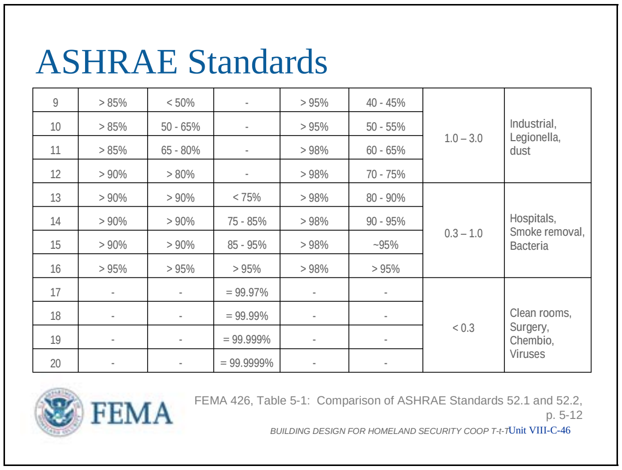
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-45

ASHRAE Standards

The new ASHRAE Standard 52.2 is a more descriptive test than ASHRAE Standard 52.1. Standard 52.2 quantifies filtration efficiency in different particle size ranges and is more applicable in determining a filter's effectiveness to capture a specific agent. Standard 52.2 reports the particle size efficiency results as a MERV rating between 1 and 20. A higher MERV rating indicates a more efficient filter.

INSTRUCTOR NOTES

VISUAL VIII-C-46



ASHRAE Standards

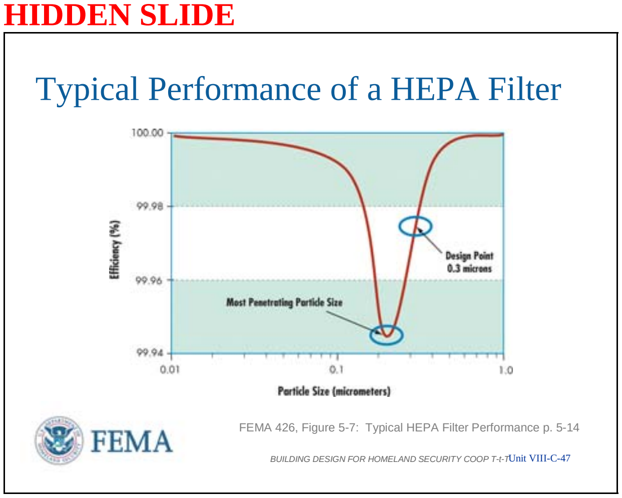
9	> 85%	< 50%	-	> 95%	40 - 45%	1.0 – 3.0	Industrial, Legionella, dust
10	> 85%	50 - 65%	-	> 95%	50 - 55%		
11	> 85%	65 - 80%	-	> 98%	60 - 65%		
12	> 90%	> 80%	-	> 98%	70 - 75%		
13	> 90%	> 90%	< 75%	> 98%	80 - 90%	0.3 – 1.0	Hospitals, Smoke removal, Bacteria
14	> 90%	> 90%	75 - 85%	> 98%	90 - 95%		
15	> 90%	> 90%	85 - 95%	> 98%	~95%		
16	> 95%	> 95%	> 95%	> 98%	> 95%		
17	-	-	= 99.97%	-	-	< 0.3	Clean rooms, Surgery, Chembio, Viruses
18	-	-	= 99.99%	-	-		
19	-	-	= 99.999%	-	-		
20	-	-	= 99.9999%	-	-		

FEMA

FEMA 426, Table 5-1: Comparison of ASHRAE Standards 52.1 and 52.2, p. 5-12

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit VIII-C-46

VISUAL VIII-C-47
HIDDEN SLIDE



CONTENT/ACTIVITY

ASHRAE Standards

The standard provides a table (depicted on the slide) that shows minimum Particle Size Efficiency (PSE) for three size ranges for each of the MERV numbers 1 through 16. Thus, if the size of a contaminant is known, an appropriate filter with the desired PSE for that particular particle size can be identified.

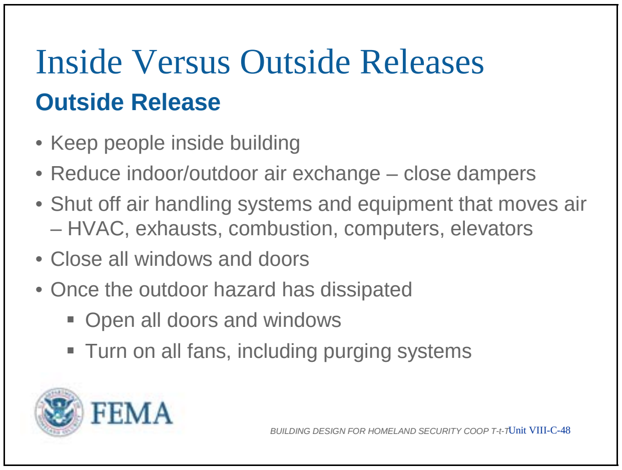
Typical Performance of a HEPA Filter

HEPA filters are typically rated as 99.97 percent effective in removing dust and particulate matter greater than 0.3 micron in size.

A typical HEPA performance curve is depicted on this slide. The dip between 0.1 and 0.3 micron represents the most penetrating particle size. Many bacteria and viruses fall into this size range. Fortunately, microbes in this range are also vulnerable to ultraviolet radiation. For this reason, many facilities couple particulate air filters with ultraviolet germicidal irradiation (UVGI). UVGI will be discussed on slide VIII-C-55.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-48



Outside Versus Inside Releases

Outside Release

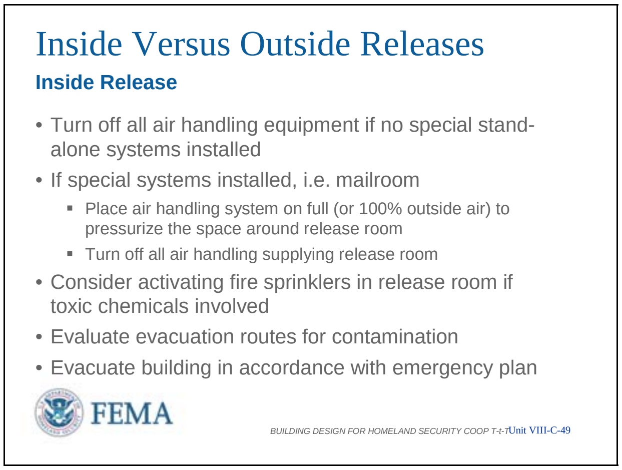
The intent is to limit exposure (dose x time) of individuals by keeping the agent and people separated to greatest extent possible. Use natural wind, sunlight, and agent material properties to allow the high-concentration plume to pass the building and minimize the agent that gets into the building.

- Keep individuals inside the building – use the building envelope as a protective enclosure
- Reduce the indoor/outdoor air exchange (seal dampers – low leakage, fast acting (much less than 30 seconds to close) dampers) to prevent contaminated air from passing through the HVAC system by normal chimney and wind effects
- Immediately shut off the air handling systems and any other system that has a fan that moves air – bathroom exhausts, combustion burners, computer cabinet cooling fans, etc. Note that elevator operation acts as a big air pump that changes air pressure throughout the building. Do not want to set up a pressure differential that pulls outside air into the building when this outside air is contaminated.
- Close all windows and doors – Should have sealed all other leakage points throughout the building envelope as part of mitigation plan
- Once the outdoor hazard has dissipated, open all doors and windows and turn on all fans to ventilate the building. While the amount of agent entering the building should be low (low dose) if you do not ventilate the building the exposure time

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

becomes great and the overall level of exposure can become dangerous.

VISUAL VIII-C-49



Outside Versus Inside Releases

Inside Release

The intent here is to keep the release contained to the greatest extent possible and prevent it from getting to the other parts of the building or outside the building.

- o This process must be well thought out, coordinated, and tested to ensure the building will function as desired.
- o If the building cannot be operated this way, then follow outside release procedures, but with evacuation.

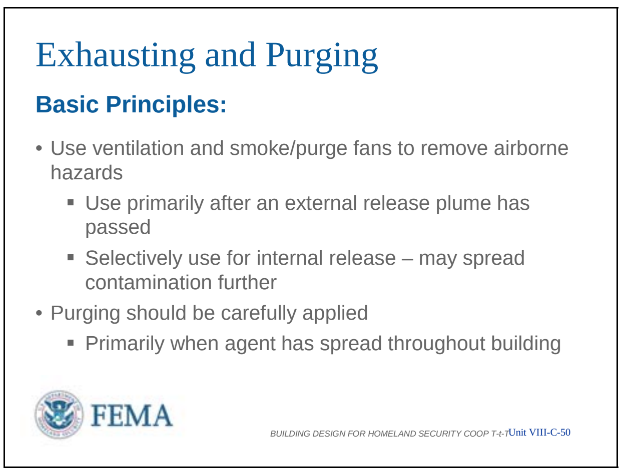
- If no special stand-alone systems, then shut down all air movement equipment
- If release is in a room with a special stand-alone system, then shut down that system and place the rest of the building's air handling system on "full (or 100%) outside air to keep the agent inside the release room.
- If advised of an in-building release of hydrogen cyanide gas, chlorine gases, or other toxic industrial chemicals, consider activating the fire sprinklers (water) to help wash the contaminant from the air stream. This would probably help for particulate aerosols like anthrax but will probably not work for vapors such as hydrogen cyanide gas or chlorine gas.
  - o The negative to this process is that the water is now contaminated and can spread throughout the building.
  - o The runoff water will also contaminate building components to a greater extent that if the sprinklers were not used, necessitating a greater clean-up effort.
  - o Note that this type of operation is not

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

standard on fire sprinkler systems and would be very difficult to implement.

- Evacuate the building in accordance with the building's emergency evacuation plan. Evacuation routes may be hazardous because they may take people through contaminated areas. It is necessary to evaluate the scenario prior to evacuating the building to prevent additional injuries from occurring.

VISUAL VIII-C-50



<u>Note: Mention that a ventilation system and smoke purge fans can be used to purge the building after an external release after the hazard outdoors has dissipated, and it has been confirmed that the agent is no longer present near the building.</u>

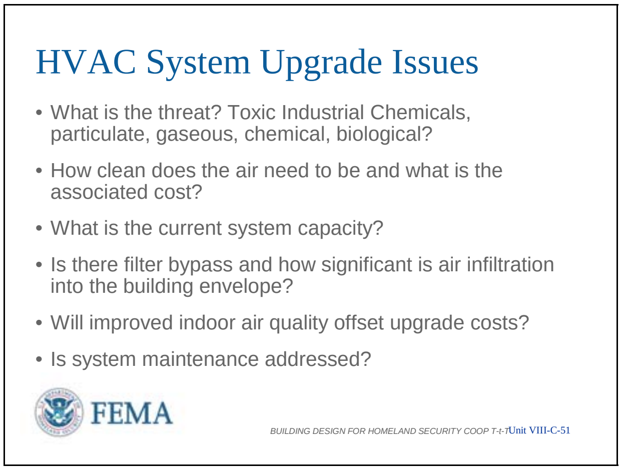
Exhausting and Purging

The fifth protective measure for CBR covered in **FEMA 426** is **Exhausting and Purging.** Turning on a building's ventilation fans and smoke-purge fans is a protective action for purging airborne hazards from the building and reducing the hazard to which building occupants are exposed.

- Purging must be carefully applied with regard to the location of the source and the time of the release. <u>The main action is final clean-out of the building to allow a return to occupancy.</u>
- <u>If the hazardous material has been identified before release or immediately upon release, purging should not be employed, because it may spread the hazardous material throughout the building, the adjacent area, and to nearby buildings.</u> In this case, all air handling units should be turned off to isolate the hazard while evacuating or temporarily sheltering in place.
- When purging, the indoor-outdoor air exchange rate can be increased by opening all windows and energizing all other fans.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

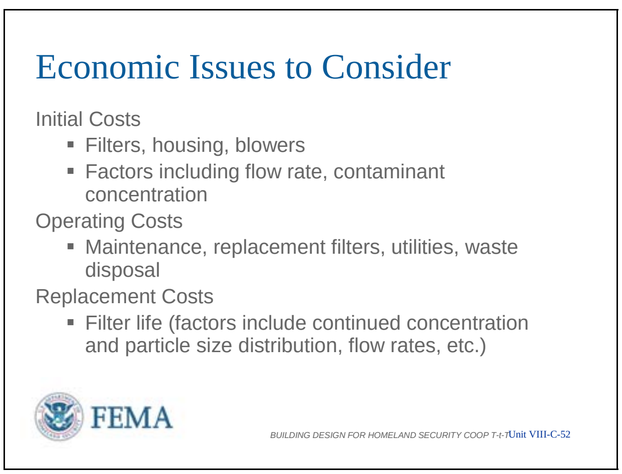
VISUAL VIII-C-51



HVAC System Upgrade Issues

- What is the threat?
- How clean does the air need to be and what is the associated cost?
- What is the current system capacity? [Cubic feet per minute (CFM) and pressure drop allowed across existing filters. Will upgraded filters result still achieving CFM required?]
- Is there filter bypass and how significant is air filtration into the building envelope?
- Will improved indoor air quality offset upgrade costs?
- Is system maintenance addressed?

VISUAL VIII-C-52



Economic Issues to Consider

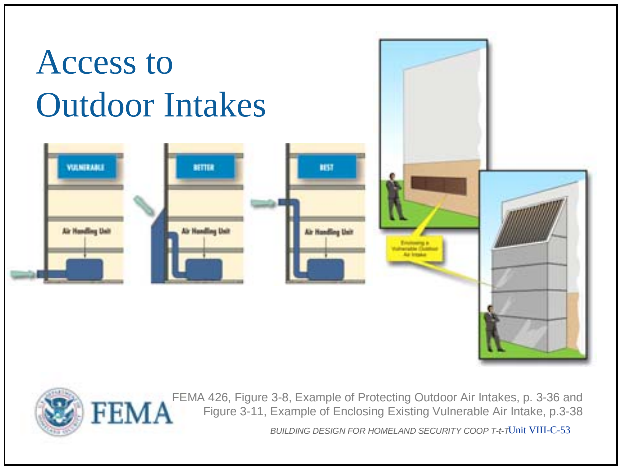
In developing, implementing, and sustaining a program to reduce vulnerability to terrorist threats, there are economic issues to consider, including three categories of costs:

- Initial costs
- Operating costs
- Replacement costs

These need to be factored into protection strategies.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-53



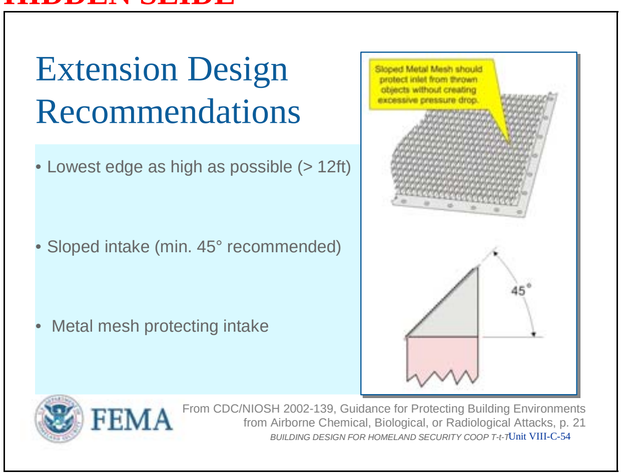
Note: The goal of this protective measure is to minimize public accessibility. In general, this means ***the higher the extensions, the bette***r—as long as other design constraints (excessive pressure loss, dynamic and static loads on structure) are appropriately considered.

Access to Outdoor Intakes

- Several <u>physical security measures</u> can be applied to reduce the potential for hazardous materials entering a building through the HVAC system.
- One of the most important steps in protecting a building's indoor environment is the <u>security of the outdoor air intakes</u>. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system.
- If relocation of outdoor air intakes is not feasible, <u>intake extensions</u> can be constructed without creating adverse effects on HVAC performance.

This is a good idea for other reasons, such as keeping grass clippings, lawnmower fumes, and/or traffic fumes from being pulled into the building because of a low intake.

VISUAL VIII-C-54
HIDDEN SLIDE

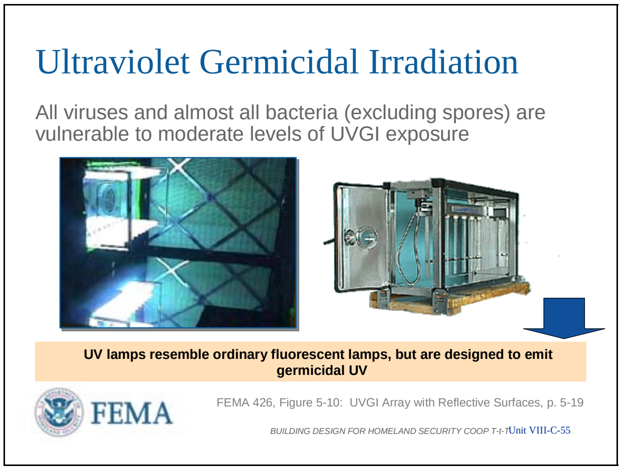


Extension Design Recommendations

An extension height of 12 feet will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes.

INSTRUCTOR NOTES

VISUAL VIII-C-55



Note: UVGI has long been used in laboratories and health care facilities. Ultraviolet radiation in the range of 2,250-3,020 Angstroms is lethal to microorganisms. All viruses and almost all bacteria (excluding spores) are vulnerable to moderate levels of UVGI exposure. Spores, which are larger and more resistant to UVGI than most bacteria, can be effectively removed through high efficiency air filtration.

Consequently, most UGVI systems are installed in conjunction with high efficiency filtration systems.

A UVGI system is being tested under the sponsorship of the Defense Advanced Research Projects Agency (DARPA). For additional information consult: http://www.novatroninc.com/technology/.

CONTENT/ACTIVITY

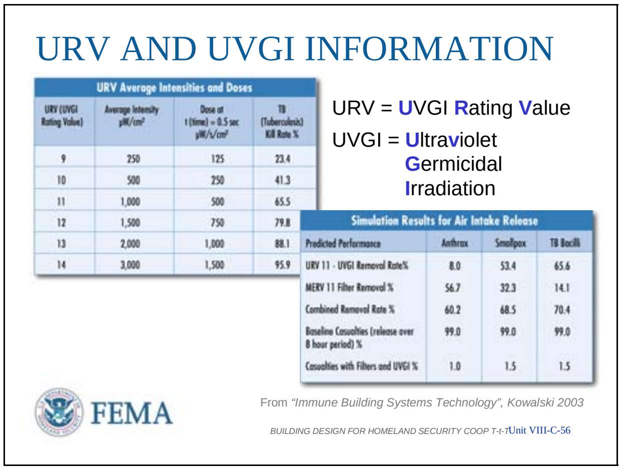
Ultraviolet Germicidal Irradiation (UVGI)

A design utilizing a combination of filtration and UVGI can be very effective against biological agents.

- Smaller microbes are difficult to filter out, but tend to be more susceptible to UVGI
- Larger microbes, such as spores, which are more resistant to UVGI, tend to be easier to filter out.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL VIII-C-56
HIDDEN SLIDE



URV Average Intensities and Doses

URV (UVGI Rating Value)	Average Intensity µW/cm²	Dose at t (time) = 0.5 sec µW/s/cm²	TB (Tuberculosis) Kill Rate %
9	250	125	23.4
10	500	250	41.3
11	1,000	500	65.5
12	1,500	750	79.8
13	2,000	1,000	88.1
14	3,000	1,500	95.9

Simulation Results for Air Intake Release

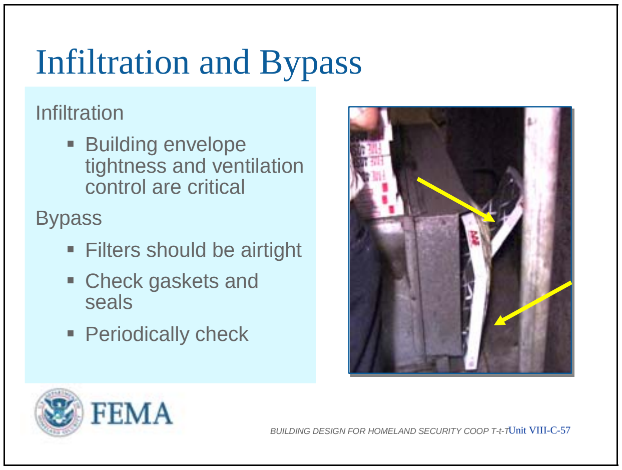
Predicted Performance	Anthrax	Smallpox	TB Bacilli
URV 11 - UVGI Removal Rate%	8.0	53.4	65.6
MERV 11 Filter Removal %	56.7	32.3	14.1
Combined Removal Rate %	60.2	68.5	70.4
Baseline Casualties (release over 8 hour period) %	99.0	99.0	99.0
Casualties with Filters and UVGI %	1.0	1.5	1.5

URV and UVGI Information

This table displays UVGI Rating Value (URV) for air disinfections systems that parallel the ASHRAE 52.2-1999 method for testing and rating filters known as MERV (minimum efficiency reporting value). The proposed URV rating system consists of 20 separate levels of average UVGI intensity.

Simulation Results for Air Intake Release
Various simulations were run in the reference shown indicating the removal rates for three design basis pathogens for MERV 11 filters, URV 11 UVGI systems, and both working together. Note the almost 100 % casualties if the agent is released into the air intake over an 8-hour period without any protective systems installed, and that about 1 % casualties occur with MERV 11 and URV 11 systems working together for the same release.

VISUAL VIII-C-57



Note: Building envelopes in residential and commercial buildings are, in general, quite leaky, and significant quantities of air can infiltrate the building envelope with minimal filtration. Field studies have shown that, unless specific measures are taken to reduce

Infiltration and Bypass

Infiltration. Building managers *should not expect filtration alone to protect a building from outdoor releases*, particularly for systems in which no make-up air or inadequate overpressure is present. Filtration, in combination with other steps, such as building pressurization and tightening the building envelope, should be considered to increase the likelihood that the air entering the building actually passes through the filtration and air-cleaning systems.

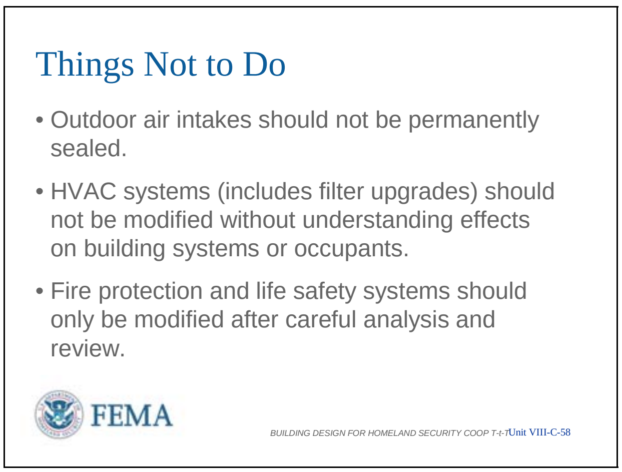
Bypass. Filter bypass is a common problem found in many HVAC filtration systems. It occurs when air, rather than moving through the filter, goes around it, decreasing collection efficiency and defeating the intended purpose of the filtration system.

INSTRUCTOR NOTES

infiltration, as much air may enter a building through infiltration as through the mechanical ventilation system.

NOTE to instructor: Emphasize to students that this slide is a good example of what looks like just poor maintenance actually creates a critical system flaw that will affect HVAC system performance in handling CBR situations. A filter is only good if ALL the air flows through it.

VISUAL VIII-C-58



CONTENT/ACTIVITY

Filter bypass is often caused by poorly fitting filters, poor sealing of filters in their framing systems, missing filter panels, or leaks and openings in the air handling unit downstream of the filter bank and upstream of the blower. Simply improving filter efficiency without addressing filter bypass provides little, if any, improvement to system efficiency. As a mechanical system loads with particulates over time, its collection efficiency increases, but so does the pressure drop.

Things Not to Do

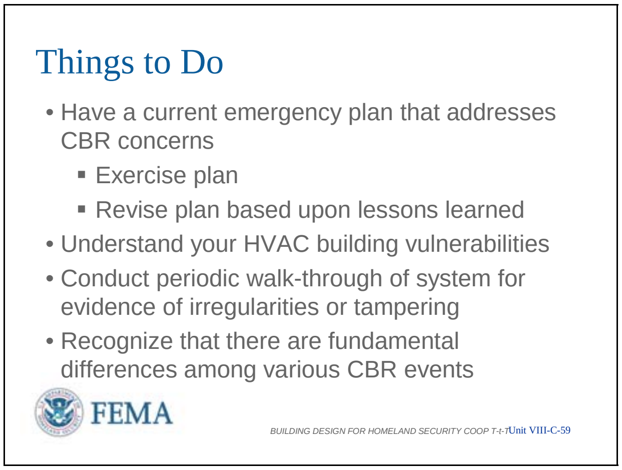
More than anything else, building owners and managers should ensure that any actions they take do not have a detrimental effect on the building systems (HVAC, fire protection, life safety, etc.) or the building occupants under normal building operation.

Some efforts to protect the building from a CBR attack could have adverse effects on the building's indoor environmental quality. This can result in higher levels of illness among building occupants, much like “sick” building situations or long distance air travel.

Building owners and managers should understand how the building systems operate and assess the impact of security measures on those systems.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL VIII-C-59



VISUAL VIII-C-60

Things to Do

Facilities managers should have a current emergency plan that addresses chemical, biological, and radiological (CBR) attacks, know their building HVAC system vulnerabilities, and conduct periodic walk-through inspections of the systems for evidence of irregularities or tampering.

Individuals developing emergency plans and procedures should recognize that there are fundamental differences among various CBR agents.

Summary

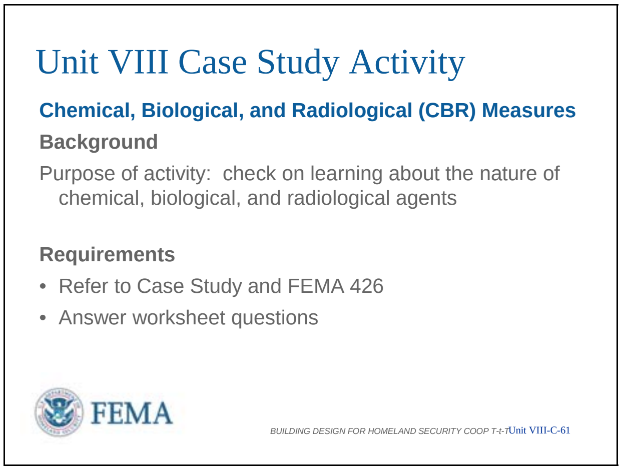
- CBR threats are real and growing.
- Industrial chemicals are readily available.
- Military chemicals require specialty expertise.
- Most buildings provide a reasonable level of protection.
- Inside versus outside building release determines evacuation decision.

Bottomline: Develop an emergency plan for CBR attacks, knowing what actions will be taken, exercise the capability and ensure it works.

At worst, a thorough CBR analysis of HVAC systems will result in good recommendations for energy conservation and proper system maintenance.

INSTRUCTOR NOTES

VISUAL VIII-C-61



Refer participants to **FEMA 426** and the Unit VIII 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 10 minutes, reconvene the class and facilitate group reporting.

CONTENT/ACTIVITY

Student Activity

This activity provides a check on learning about the nature of chemical, biological, and radiological agents.

Activity Requirements

Working in your small groups, refer to the CI/BC Case Study and **FEMA 426** to answer the worksheet questions.

Take 10 minutes to complete this activity. Solutions will be reviewed in the plenary group.

Transition

This completes the background information in Units I through VIII. The next three units will cover vulnerabilities and mitigation measures.

Unit IX will cover Site and Layout Design Guidance.

This page intentionally left blank

**UNIT VIII (C) CASE STUDY ACTIVITY:
CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL (CBR) MEASURES
(COOP Version)**

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

Requirements

1. Identify the prevalent CBR threat(s) that exist and/or are identified as the Design Basis Threat in the Case Study.

Appendix C: Cooperville Information / Business Center

Design Basis Threat

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

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

Radiological: ***Small "dirty" bomb detonation within the 10-mile radius of the CI/BC building.***

Other:

Chemical:

1) ***There are a significant number of hazardous waste sites in near proximity to the CI/BC building. The vast majority are small generators such as gas stations, dry cleaning, and other commercial businesses.***
2) ***CI/BC is surrounded by a number of commercial activities and key national critical infrastructure to include Hazardous Material (HazMat) facilities, HazMat being transported on the roads and rails, a nearby fuel tank farm, and an airport.***
3) ***There are two large manufacturing plants with large quantities of hazardous materials stored on site within 2 miles of the CI/BC Headquarters, one to the north and the other to the southwest. In addition, there are more than a dozen Tier II HazMat facilities within 3 miles of the building (in all directions)***
4) ***Approximately 5,000 trucks per day pass the CI/BC office on the nearby interstate highway. About 30 percent of these trucks (1,500 trucks/day) carry placards indicating that HazMat is aboard, but only about 5 percent (250 trucks/day) carry sufficient HazMat to warrant placarding.***
5) ***Approximately 50 percent of the HazMat passing the CI/BC office is Class 3 (flammable and combustible liquids). Class 2 (gases) and***

Class 8 (corrosives) each constitute about 15 percent. Approximately 10 percent of the trucks carry more than one class of HazMat.

6) ***It is estimated that approximately 10,000 railcars of HazMat move through this area each year. Hazardous materials range from liquid petroleum products to chlorine to anhydrous ammonia.***
7) ***A leg of the Piedmont Petroleum Pipeline (PPP) runs underneath the office park in the vicinity of CI/BC Headquarters. Part of Piedmont's regional network, this portion of the pipeline normally carries a variety of refined products, including commercial and military jet fuels, diesel and three grades of gasoline, home heating fuels, etc. Four buried pipes carry approximately 20 million gallons per day.***
8) ***Connected to the pipeline, less than 1 mile from CI/BC, is a 20-million gallon capacity fuel farm. Operated by the Shellexxico Company, this tank farm stores a variety of petroleum products, primarily gasoline. Thirteen tank trucks were observed leaving the tank farm in a 1- hour period, indicating a calculated movement rate of approximately 300 trucks per day (about 3 million gallons of fuel).***

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

2. What size filtration unit (MERV) is required to filter out 80 percent of Legionella and dust particulates (1 to 3 microns)? ***12***

3. What range of MERV is required to remove 85 percent of smoke particles greater than 0.3 micron in size? ***15 or higher***

4. What mitigation measure can be used in HVAC system to destroy bacteria and viruses? ***UVGI lamps***

Unit IX (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 150 minutes
UNIT TITLE	Site and Layout Design Guidance
OBJECTIVES	1. Identify site planning concerns that can create, reduce, or eliminate vulnerabilities and understand the concept of "Layers of Defense." 2. Recognize protective issues for suburban site planning. 3. Compare the pros and cons of barrier mitigation measures that increase stand-off or promote the need for hardening of buildings at risks. 4. Understand the need for keeping up with the growing demand for security design. 5. Understand the benefits that can be derived from appropriate security design. 6. Understand the benefits of adopting a creative process to face current design challenges. 7. Understand the benefits of including aesthetic elements compatible with security and architecture characteristics of building and surrounding environment. 8. Apply these concepts to an existing site or building and identify mitigation measures needed to reduce vulnerabilities.
SCOPE	The following topics will be covered in this unit: 1. Land use considerations both outside and inside the property line. 2. Site planning issues to include site design, layout and form, vehicular and pedestrian circulation, and landscape and urban design. 3. Creating stand-off distance using perimeter controls, non-exclusive zones, and exclusive zones along with the design concepts and technology to consider. 4. Design considerations and mitigation measures for site security.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings,* Chapter 2; Checklist at end of Chapter 1
2. FEMA 430, *Site and Urban Design for Security*
3. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 5-1 to 5-16
4. Case Study – Appendix C: COOP, Cooperville Information / Business Center
5. Student Manual, Unit IX (C) (info only – not listed in SM)
6. Unit IX (C) visuals (info only – not listed 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 IX (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit IX (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

UNIT IX (C) OUTLINE

9. Second Layer, Yards and Plazas	7.5 minutes	IG-IX-C-26
10. Second Layer, Roadways	1.5 minutes	IG-IX-C-29
11. Second Layer, Parking	9 minutes	IG-IX-C-29
12. Second Layer, Signage	1.5 minutes	IG-IX-C-33
13. First/Second Layer, Security Lighting	1.5 minutes	IG-IX-C-34
14. First Layer, Sensors/CCTV	1.5 minutes	IG-IX-C-35
15. Second Layer, Site Utilities	4.5 minutes	IG-IX-C-35
16. Best Practices	4.5 minutes	IG-IX-C-37
17. Activity: Site and Layout Design Guidance (Version **(C) COOP**) [45 minutes for students, 15 minutes for review]	60 minutes	IG IX-C-39

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** This is a generic instruction unit, but it has great capability for linking to the Local Area. Local Area discussion may be generated as students have specific situations for which they would like to determine vulnerabilities or vulnerability rating prompted by points brought up in the presentation.

- **Optional Activity:** There is no optional activity for this unit.

- **Activity:** The students will continue familiarizing themselves with the Case Study materials. The Case Study is a risk assessment and analysis of mitigation options and strategies for an alternate facility to be assessed for potential Continuity of Operations (COOP). This alternate facility is a typical commercial office building located in a mixed urban-suburban environment business park. The assessment uses the DoD Antiterrorism Standards and the GSA Interagency Security Criteria to determine Levels of Protection and identify specific vulnerabilities. Mitigation options and strategies will use the concepts provided in **FEMA 426** and other reference materials.

- Refer students to their Student Manual for worksheets and activities.

- Direct students to the appropriate page (Unit #) in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- "Walk through" the pages of the activity with the students, describing the steps followed to obtain the answers in the completed examples, and what is expected of the groups for this activity.

- For this activity, the assessment of the site and layout of the building in greater depth may result in the group adjusting the Risk Matrix scores for vulnerability rating, with resultant changes to risk rating. Transfer these changes 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 checklist section of questions, in summary fashion or select representative questions in each section as the starting points of discussion. 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. Note, there are no right or wrong answers, but all answers must be justified with rationale.

- Ask for and answer questions.

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

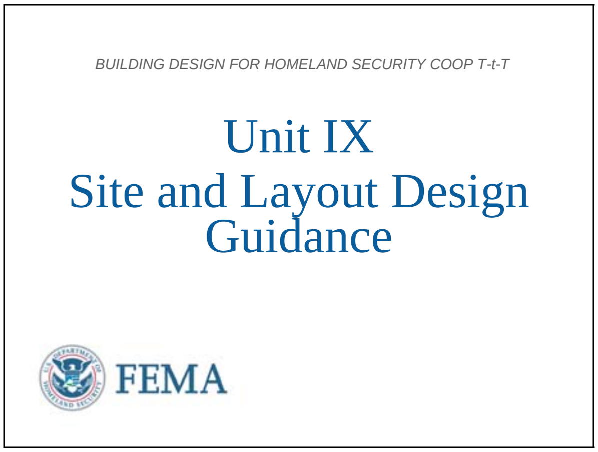
(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

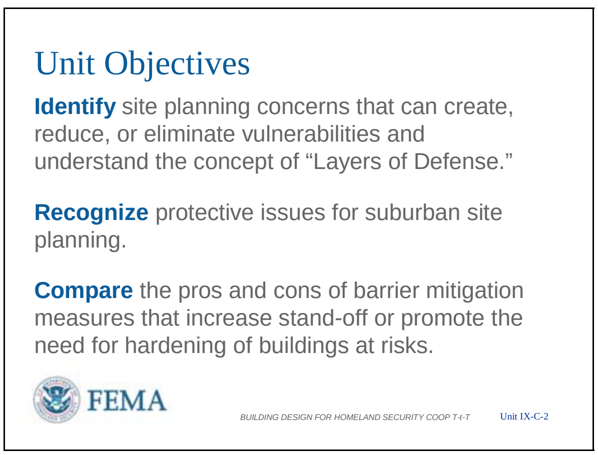
Unit IX-C-1



Introduction and Unit Overview

This is Unit IX, Site and Layout Design Guidance. This lecture will examine site level considerations and concepts for integrating land use planning, landscape, architecture, site planning, and other strategies to mitigate the design basis threats. The students will gain an understanding of the myriad options available to enhance site design taking into account many environmental challenges.

Unit IX-C-2



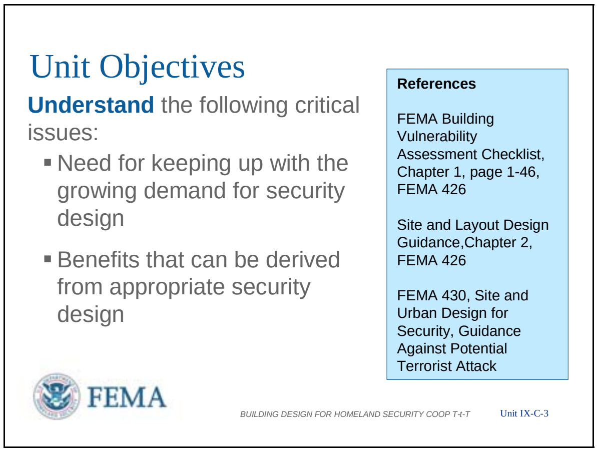
Unit Objectives

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

1. Identify site planning concerns that can create, reduce, or eliminate vulnerabilities and understand the concept of "Layers of Defense."
2. Recognize protective issues for suburban site planning so as to aid in selecting appropriate mitigation measures.
3. Compare the pros and cons of barrier mitigation measures that increase stand-off and the need for hardening buildings at risk.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

Unit IX-C-3

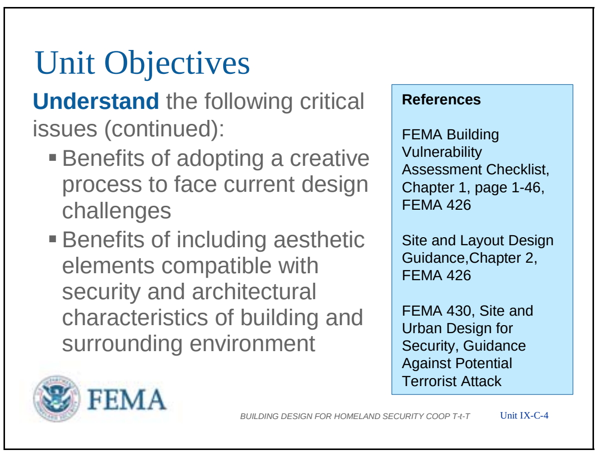


Unit Objectives (cont.)

5. Understand the benefits in keeping up with the growing demand for security design issues. The technology and manufacturing continues to improve.
6. Understand the benefits that can be derived from appropriate security design. Meeting security design can satisfy other requirements at the same time.

FEMA 426 and FEMA 430 contain architectural and site planning considerations for new design or renovation of existing.

Unit IX-C-4

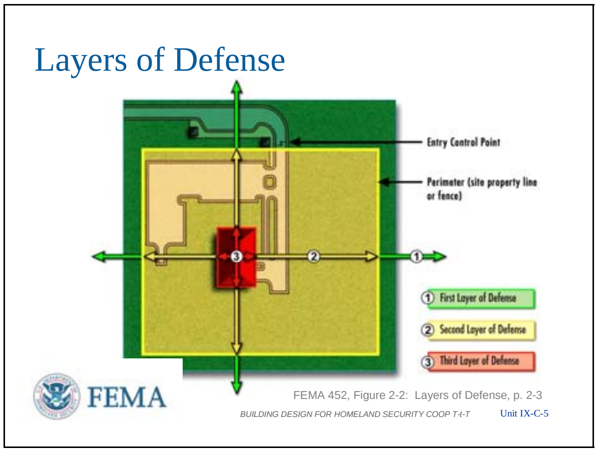


Unit Objectives (cont.)

7. Understand that there are benefits to adopting a creative process to face current design challenges. While many criteria are prescriptive, there are many techniques to meet the spirit, intent, purpose, and performance sought.
8. Understand that design can include aesthetic elements that are compatible with security and architectural characteristics of the building and surrounding environment. Blending security so that it does not look like security and buildings feel open and friendly should be a goal.

INSTRUCTOR NOTES

Unit IX-C-5



From FEMA 452

The layers of defense is a traditional approach in security engineering and use concentric circles extending out from an area or site to the building or asset that requires protection. They can be seen as demarcation points for different security strategies. Identifying the layers of defense early in the assessment process will help you to understand better the assets that require protection and determine your mitigation options. Figure 2-2 shows the layers of defense described below.

First Layer of Defense. This involves understanding the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of adjacent activities. It is specifically concerned with buildings, installations, and infrastructure outside the site perimeter. For urban areas, it also includes the curb lane and surrounding streets. **The building owner has little or no control outside of working with the city or municipality. The first layer of defense should be designed to prevent large bombs or weapons into the site and control access**

CONTENT/ACTIVITY

Layers of Defense

There should always be multiple layers of defense in order to deter and detect potential threat elements that attempt to access critical assets to their benefit and everyone else's detriment. There may be an additional layer applied around a building when a site is large or one or more additional layers inside a building when a building has functions at various levels of security. The intent is to deter first, then detect sufficiently quickly to have a response force engage the potential threat elements prior to reaching the next layer.

The first layer is the demarcation between control and no control. Outside the first layer the local, regional, and national police and intelligence forces work to track, detain, and arrest the potential threat elements before they can initiate an incident. This should be a controlled perimeter whose intent is to keep large threats outside by deterrence or detect them at this point and prevent entry. If the weapon activates at this layer the effectiveness is reduced if sufficient stand-off exists.

The second layer keeps any smaller weapons that may slip past the first layer from getting close enough to the critical asset to cause damage. This layer should mitigate the effectiveness of tactics, reduce the impact due to insider action, and controls the stand-off from the building for the smaller weapons that may get through.

The first and second layers are primarily the venue for site and layout design, the basis for this unit.

The third layer (usually 3 layers are the minimum found) is the building envelope which also deters and detects, but if an incident occurs this layer is the only one that provides

of personnel.

Second Layer of Defense. This refers to the space that exists between the site perimeter and the assets requiring protection. It involves the placement of buildings and forms in a particular site and understanding which natural or physical resources can provide protection. It entails the design of access points, parking, roadways, pedestrian walkways, natural barriers, security lighting, and signage. For urban areas, it refers specifically to the building yard. **The building owner has control of this layer. The second layer controls stand-off from the building which provides protection from weapons that may slip through the first layer of defense.**

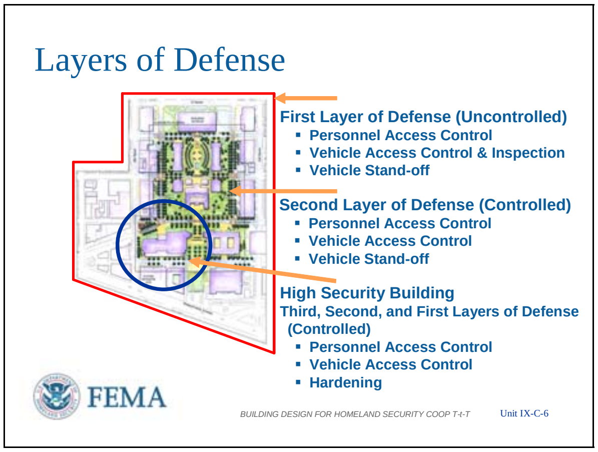
Third Layer of Defense. This deals with the protection of the asset itself. It proposes to harden the structures and systems, incorporate effective HVAC systems and surveillance equipment, and wisely design and locate utilities and mechanical systems. Note that, of all blast mitigation measures, distance is the most effective measure because other measures vary in effectiveness and can be more costly. However, often it is not possible to provide adequate stand-off distance. For example, sidewalks in many urban areas may be less than 10 meters (33 feet), while appropriate stand-off may require a minimum of 25 meters (82 feet). **The building owner has control of this layer and its main mitigation measures are hardening against blast and security sensors/CCTV as final access control.**

any level of protection during the tactic and weapon release. The third layer is the venue for building design which will be found in the next instruction unit.

It is important to remember that the nature of any threat is always changing. Consideration should be given to accommodating enhanced protection measures in response to future threats that may emerge. Asset protection must be balanced with other design objectives, such as the efficient use of land and resources, and must also take into account existing physical, programmatic, and fiscal constraints.

INSTRUCTOR NOTES

Unit IX-C-6



The layers of defense are not predetermined and they may vary from site to site and from building to building. If a particular building requiring protection is part of a campus or located in a rural, semi-rural, or urban area, a similar analysis may be applicable for all cases when determining the importance of the asset. However, the security elements necessary to protect the building can be entirely different, depending on its location. The approach suggests establishing different demarcation points in order to identify sound security strategies. The layers of defense concept proposes that each designer study a particular site and determine critical assets that need to be protected and how protection should take place.

Note: Layers of Defense will be during this and the next two instruction units to illustrate the elements:

- Deter
- Detect
- Deny
- Devalue

CONTENT/ACTIVITY

Layers of Defense

The layers of defense convey the idea of using concentric circles extending out from an area or site to the building that requires protection. They are used as demarcation points for different security strategies. The objective of layers of defense is to create succeeding more difficult layers to security to penetrate, provide additional warning and response time, and allow building occupants to more into defensive positions or designated Safe Haven protection.

The layers of defense defines sites and projects as follows *(While the previous slide is a generic explanation, this slide shows the campus or suburban situation where there are more options to the layers of defense)*:

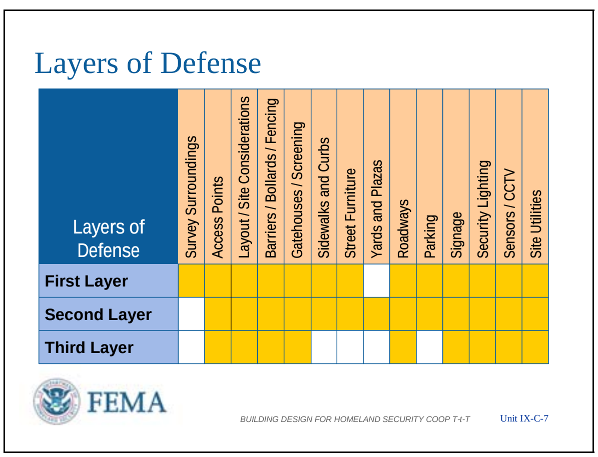
- The first layer addresses the characteristics of the surrounding area and the public realm. It starts at the site perimeter and outward. The building owner has very limited or no control to implement mitigation measures.
- Although a controlled access zone is one of the best methods of ensuring stand-off, issues as the size of site, site limitations, building siting within the parcel, and property line restrictions do not always allow this zone to be created.
- The second layer is concerned with the space and physical barriers at the perimeter of the site to keep explosives at a distance to protect buildings. It comprises the space between the site perimeter and building. The building owner has the authority and control to implement mitigation measures.
- The third deals with the protection integral to the building itself. The building owner has certain level of control to implement mitigation measures. Incorporating the protection in initial design, whether blast hardening or security, is the least expensive approach. Retrofitting after the building has

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

been constructed can cost up to 30% of the original construction, if the retrofitting can be done.

Instructors may want to relate to a castle – First layer of defense is clearing all trees and vegetation out to the effective range of arrows and crossbows. Second layer of defense is moat and initial castle wall. Third layer of defense is the castle keep where the last defensive position exists with its additional walls.

Unit IX-C-7



Layers of Defense

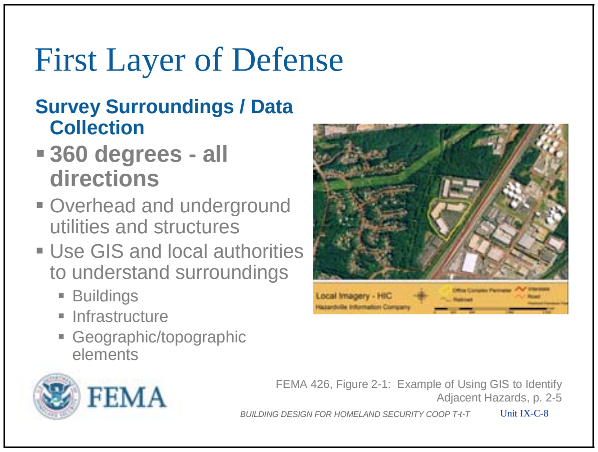
There are many mitigation techniques available that can be used at one or more layers of defense. This instruction unit concentrates on site and layout design, thus it looks primarily at the first and second layers of defense and emphasizes the predominant layer of defense considered.

Here are general mitigation considerations for the suburban environment and this presentation will follow the flow of these measures from left to right – starting with Survey Surroundings on the left and ending with Site Utilities on the right.

The flow also follows the general assessment approach of looking from outside to inside and going from general information to specific information.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

Unit IX-C-8



NOTE to instructor: Emphasize that a **360 degree survey of surroundings** must be done as you cannot ignore what is overhead or underground. Also, the FEMA 452 database has questions specifically targeting these concerns under Site and Sturctural. (These questions are **not yet in** FEMA 426 or FEMA 452.)

Survey Surroundings – Data Collection

In a suburban environment, this action normally follows the points on a compass -- in the horizontal plane.

However, understanding the surroundings includes any structures above and under the building and site of interest as to their impact on design or assessment. GIS applications are excellent resources that enable designers and building owners to analyze various demographic, hazardous areas, transportation networks, access control points, etc., in order to identify potential threats, hazards, and vulnerabilities. These applications may depict a truer picture of the surrounding situation, allowing decision-makers to take proactive measures to mitigate potential vulnerabilities.

Geographic and topographic concerns include terrain that limits access of vehicles – natural barriers, like water, slope, vegetation, etc.

Unit IX-C-9

Access Points

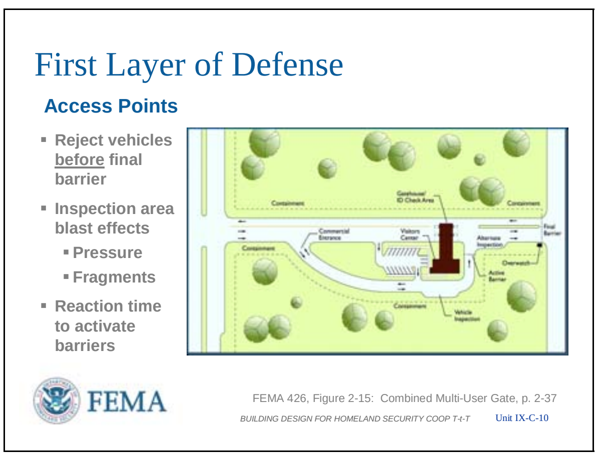
Entry control and vehicular access should:

- Prevent unauthorized access
- Avoid traffic queuing (queues become potential targets)
- Have commercial vehicle gates if possible – keep larger vehicles further away and barriers increased in capability to handle. Have an Alternate Plan B if a suspected vehicle closes down one or the other vehicle gates
- Provide traffic calming
- Avoid high speed approaches
- Have equal security capacity for exit

Traffic calming strategies seek to use design measures to cue drivers as to the acceptable speed for an area. These include raised

INSTRUCTOR NOTES

Unit IX-C-10



Location selection for vehicular access and entry control for a building starts with an evaluation of the anticipated demand for access to the controlled site. An analysis of traffic origin and destination, and an analysis of the capability of the surrounding connecting road network, including its capacity to handle additional traffic, should then be performed. Expansion capacity

CONTENT/ACTIVITY

crosswalks, speed humps and speed tables, pavement treatments, build outs, and traffic circles. Additionally, by controlling the angle of approach, requiring turns or providing curves, vehicles must slow down.

The arrival sequence design to and through a site contribute to the project's identity, including the visitor's orientation to the site and route to reach their destination. The circulation routes, signage, checkpoints, control of site lines (screening or emphasizing views of certain areas), and topography all contribute to the arrival process and legibility of the site. The establishment of circulation and access points may differentiate between entries and routes for pedestrians, staff, visitors, deliveries and service, each with differing security requirements to be satisfied.

Access Points

Gatehouses, lobbies, and guard posts should be provided with clear views of approaching traffic -- pedestrian and vehicular. Screening areas and entries may be located to offer more privacy and protection.

It is advisable to design circulation to separate different types of traffic and provide separate routes for staff, for visitors, and for deliveries. With the separation of vehicle types, security can more easily address differing needs for screening, observation, and potential threat mitigation.

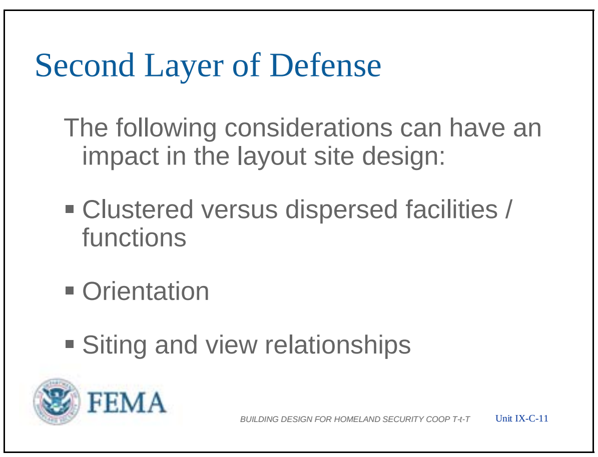
Roadway network design that uses straight-line approaches to buildings may give approaching vehicles the opportunity to gather the necessary speed to ram protective barriers and crash into buildings. Possible solution: design approaches to be parallel to the façade, with berms, high curbs, trees, and other measures used to prevent vehicles from departing the

INSTRUCTOR NOTES

should also be considered. The analysis should be coordinated with the state and local departments of transportation.

Two security measures that are overlooked are: <u>First</u>, allowing the vehicle to enter the site so that it can turn around and leave. A proper entry control point would never allow the vehicle to enter the site if it were not authorized. <u>Second</u>, there are multiple reaction times that must be added – guard recognition that vehicle is avoiding security, guard reaction to activate final barriers, and activation time from closed to open for the final barriers. The time delay from recognition to deployment must be less than the speed of the vehicle between the recognition point and the final barrier.

Unit IX-C-11



CONTENT/ACTIVITY

roadway.

The existing terrain can have a significant impact on the suitability of a potential entry control point site. Flat terrain with no thick vegetation is generally preferred. A gentle rise in elevation up to the entry control guard building allows for a clear view of arriving vehicles. Consider how existing natural features such as bodies of water or dense tree stands may enhance perimeter security and vehicle containment, without restricting observation capability or allowing easier surveillance of the building by potential threat elements. Entry control spatial requirements vary, depending on the type, the traffic demand, and the necessary security measures.

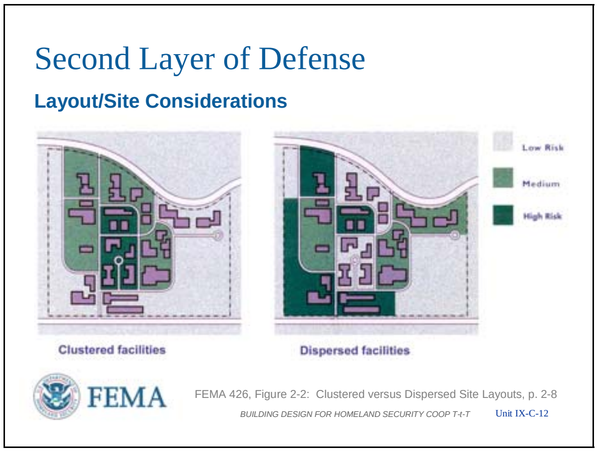
Second Layer of Defense

The following aspects of the building program and layout impact the site design and assessment:

- Overall size and number of structures placed on site with high-risk buildings clustered together for increased security or stand-off or dispersed to devalue as a target.
- Orientation of buildings to reduce damage from bomb blast and prevent direct approaches by high speed vehicles.
- Increase views of approaches to the building, but screen views from outside surveillance.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Unit IX-C-12

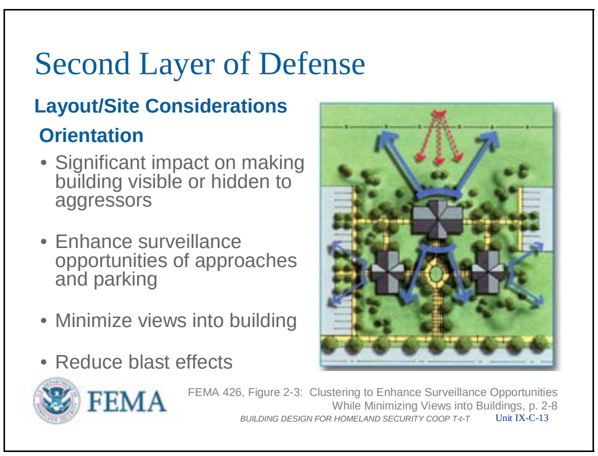


Layout / Site Considerations – Clustered versus Dispersed Facilities

Depending on the site characteristics, the occupancy requirements, and other factors, buildings may be clustered tightly in one area, or dispersed across the site. Both patterns have compelling strengths and weaknesses.

Concentrating people, property, and operations in one place creates a target-rich environment, and the mere proximity of any one building to any other may increase the risk of collateral impacts. Additionally, the potential exists for the establishment of more single-point vulnerabilities in a clustered design than would exist in a more dispersed pattern. However, grouping high risk activities, concentrations of personnel, and critical functions into a cluster can help maximize stand-off from the perimeter and create a “defensible space.”

Unit IX-C-13



Layout / Site Considerations -- Orientation

Orientation is the building’s spatial relationship to the site, its orientation relative to the sun, and its vertical or horizontal aspect relative to the ground.

- How many times have you seen aluminum foil on windows because the afternoon summer sun overcomes the air-conditioning capacity along that side of a building?

The physical positioning of a building relative to its surroundings may seem subtle, but can be a greater determinant of security.

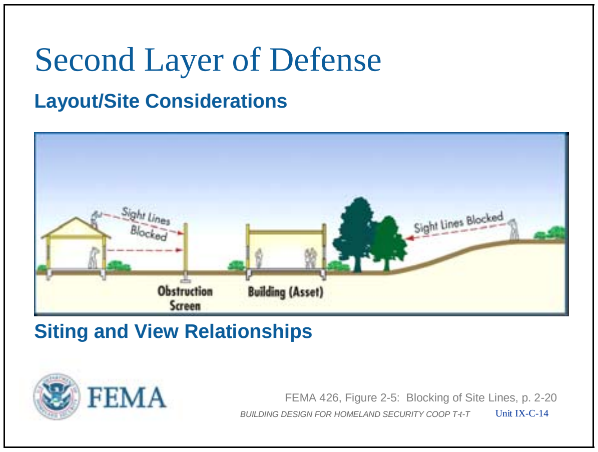
Good site design, orientation, and building placement should allow building occupants to look out of the facility while minimizing views into the building.

The proximity of a vulnerable façade to a parking area, street, adjacent site, or other area

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

that is accessible to vehicles and/or difficult to observe can greatly contribute to its vulnerability.

Unit IX-C-14



Layout / Site Considerations – Siting and View Relationships

Landscape and urban design inherently define the “line of sight” in a space. Operational security is not a traditional element of master planning, but managing the threat of hostile surveillance is a significant consideration in protecting people, property, and operations. With careful selection, placement, and maintenance, landscape elements can provide visual screening that protects sensitive operations, gathering areas, and other activities from surveillance without creating concealment for covert activity.

These techniques seek to deny aggressors a “line of sight” to a potential target, either from on or off site. This increases the protection of sensitive information and inhibits operation of stand-off weapons. In addition to the use of various screening options, anti-surveillance measures (e.g., building orientation, landscaping, screening, and landforms) can also be used to block sight lines.

The design should maximize opportunities for internal surveillance of site perimeters and screening of internal areas from external observation. Topography, relative elevation, walls, and fences are design elements that can open and close views. Vegetation can open, close, or block views, not only for security purposes but also to provide beauty and to support wayfinding. As a rule of thumb, vegetation should be very high or very low, to keep views open. Vegetation at the base of buildings and structures should be designed and maintained to prevent explosives from being hidden from view – easily see a briefcase

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

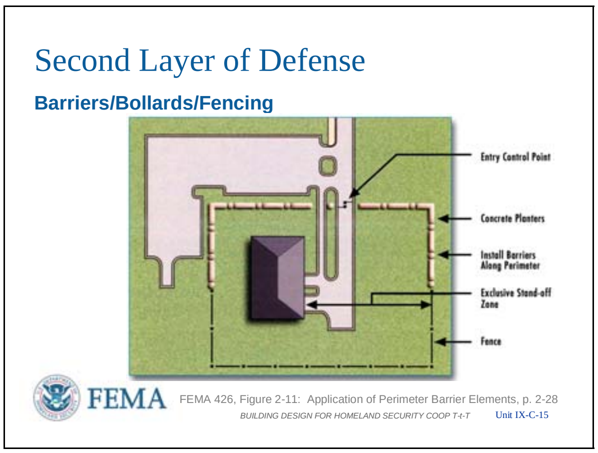
or a backpack.

Landforms can have a direct bearing on the security of a facility. They can be either beneficial (e.g., an elevated site that may enhance the surveillance of the surrounding area), or detrimental to anti-surveillance.

Generally speaking:

- For security purposes, buildings should not be sited immediately adjacent to higher surrounding terrain or buildings if at all possible.

Unit IX-C-15



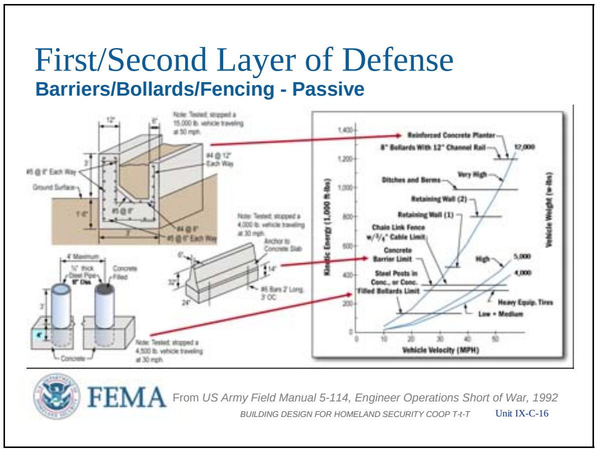
Barriers / Bollards /Fencing

A number of elements may be used to create a physical barrier, some natural and some manmade. Natural barrier elements include rivers, lakes, waterways, steep terrain, mountains, barren areas, plants, soft sand, and other terrain features that are difficult to traverse. Manmade elements include fencing, walls, buildings, bollards, planters, concrete barriers, and fountains. Selection of elements must consider the level of security desired and the type of threat most likely to occur.

When placing bollards, make sure you adhere to ADA (Americans with Disabilities Act) compliance.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Unit IX-C-16
Hidden Slide



Discuss the mass (vehicle size) and vehicle speed in the chart. Note that since speed is squared (K.E. = ½ * mass * speed * speed), controlling speed is a primary concern.

Barriers / Bollards /Fencing – Passive Barriers

It is one thing to provide a passive barrier, it is another to ensure the barrier will provide the protection level sought. We have talked about controlling vehicle speed approaching access points and buildings. Essentially, any barrier will stop a given level of kinetic energy which is ½ mass * velocity squared. Thus, the bigger the vehicle and the higher its speed the stronger the barrier must be as shown by this chart.

The greater the barrier mass and reinforcement and the deeper it is connected to the earth, the higher its rating.

Notice the jersey barrier has the rating listed only if there are four rebar pinning the barrier at least 18 inches into pavement. Alternately, a 1-inch steel cable linking the jersey barriers would be an alternate technique, but with some penetration into the space being protected.

Unit IX-C-17

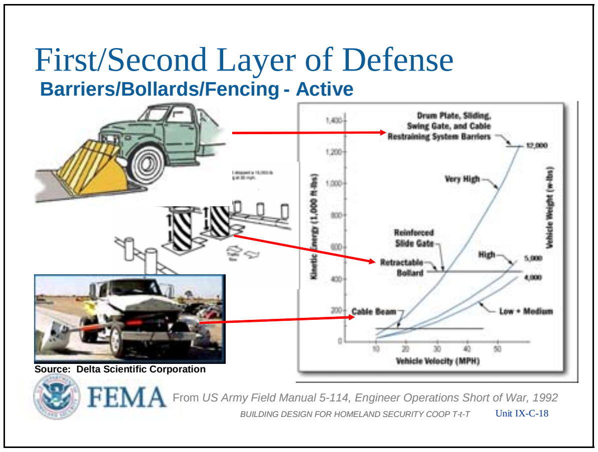
Barriers / Bollards /Fencing – Water Barriers

Water-filled barriers are another approach as they are lightweight and easy to deploy. The left photo shows the stopping power and the right photo shows water barriers that support a fence. Filling the barriers with sand make them less portable.

As with jersey barriers, linking the barriers with 1-inch steel cable improves their performance, due to the added mass of adjacent barriers contributing to stopping the vehicle. Also, these barriers must be checked periodically for leaks, especially if allowed to freeze when filled with water. Without water or sand these would lack critical needed mass.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

Unit IX-C-18
Hidden Slide



Barriers / Bollards /Fencing – Active Barriers

As with passive barriers, active barriers also have different levels of kinetic energy stopping power, based upon mass and connection to the earth.

The advantage of active barriers is that access points and building access to loading docks or for maintenance can allow vehicles to pass or not pass based upon authorization.

One company is marketing a turntable that allows the fixed bollards to be turned 90 degrees to the vehicle path, then rotated back to block vehicle traffic.

Unit IX-C-19

Barriers / Bollards /Fencing – Active Barriers

These photos show retractable bollards stopping a substantial truck with very little penetration.

An active barrier can be activated in seconds (1 to 3) and should be either always up (sally port concept) or deployed upon identification that the gate is being crashed (taking into consideration response time, maximum vehicle speed and activation speed/time.

Pop-up barriers can create serious damage to vehicles, especially if deployed when a vehicle is above the barrier. Consider manual activation to avoid unnecessary damage (avoid magnetic vehicle loops to redeploy a barrier that will catch a tailgating vehicle).

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

Unit IX-C-20

Barriers and Street Closure

In alleys and typical urban streets adequate stand-off distance is an impossibility without street closure. This is generally undesirable because of the disruption caused to traffic patterns.

The top and left photos show permanently installed barriers, while the bottom right photo shows temporary barriers that can be rapidly deployed and moved into position to control site and parking access, control traffic flow, and provide stand-off distance for buildings.

Improvised closures tend to destroy the attractiveness of the street with a combination of security personnel and ugly temporary barriers. Configuration for access, queuing, and inspection shout be planned in any case to reduce potential problems by reducing circulation and aggregated space in a city.

Full closure is often impossible because of the need for service entry. Temporary closure can be achieved by active or manual barriers, combined with public works and security personnel.

Consider the “Ring of Steel” being installed in a core area of London, England. It acts as a first layer of defense, inspecting, restricting, and documenting all vehicles that enter the core area to keep larger weapons out.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Unit IX-C-21

First/Second Layer of Defense

Barriers, Bollards, and Fencing

Department of State periodically issues list of manufacturers and model numbers certified in meeting prescribed testing criteria (March 2003)

Rating	Vehicle Weight (lbs.)	Vehicle Speed (mph)	Distance Past Barrier (ft)
K4	15,000	30	<= 3.3
K8	15,000	40	<= 3.3
K12	15,000	50	<= 3.3

Check site utilities, water runoff, and other subterranean conditions when installing bollards and barriers

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IX-C-21

Department of State Barrier Ratings

Department of State barrier ratings are probably more suitable to an urban environment where stand-off is limited -- the 3.3 feet distance allowed past the barrier is for the leading edge of the cargo area of the truck (where the bomb is most likely being carried).

Also, Department of State has found that diesel trucks have greater penetration capability, so their tests now require the use of diesel trucks vice gasoline powered trucks.

Unit IX-C-22
Hidden Slide

First/Second Layer of Defense

Barriers, Bollards, and Fencing

Department of Defense periodically issues list of manufacturers and model numbers certified in meeting prescribed testing criteria (August 2003)

Vehicle Weight (lbs.)	Vehicle Speed (mph)	Distance Past Barrier (ft)
15,000	30	<=3(L3)/20(L2)/50(L1)
15,000	40	<=3(L3)/20(L2)/50(L1)
15,000	50	<=3(L3)/20(L2)/50(L1)
10,000	50	0 to 50
10,000	15	50 to 100

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IX-C-22

Department of Defense Barrier Ratings

Department of Defense barrier ratings use the old Department of State criterion that allows the front of the vehicle to penetrate a given distance past the barrier. This would be more suitable in a suburban environment where there is greater distance between the barrier and the nearest building than in the urban environment.

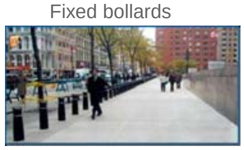
Unit IX-C-23

First/Second Layer of Defense

Barriers, Bollards, and Fencing

- Fixed bollards
- Retractable bollards
- Planters

Fixed bollards



FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IX-C-23

Barriers / Bollards /Fencing – Bollards and Planters

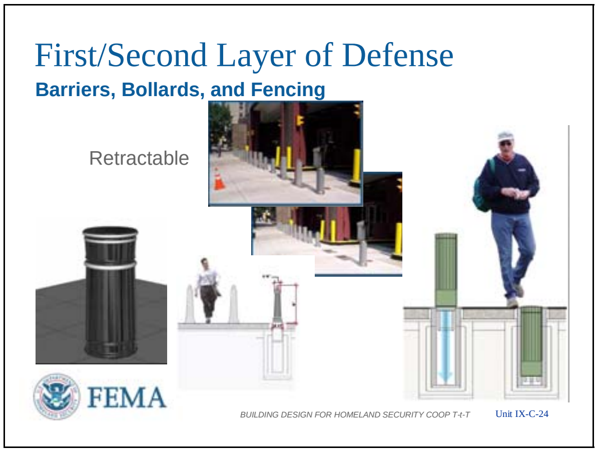
Sidewalks serve as the common space for pedestrian interaction, movements, and activity.

Extending barriers into sidewalks, streets or parking lanes may provide additional stand off distance. While this is technically possible, this approach often creates negative impacts within the public realm, which may make this an unfeasible solution. Be sure that introduced security measures are effective.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Bollards and other barriers are ideally the first layer of defense in the urban environment so as to obtain the most stand-off possible.

Unit IX-C-24



Barriers / Bollards /Fencing -- Retractable Bollards

Retractable bollards are an excellent (though expensive) solution when the use of security elements is critical and the width of the street does nor allow their permanent placement.

Effective bollards must be carefully engineered with deep foundations and the additional depth required for retracting may cause problems with underground utilities and services, building basements extending under sidewalks in urban areas, and other structures that may exist under sidewalks that affect retractable bollard performance.

Unit IX-C-25

Barriers / Bollards /Fencing -- Planters

Bollards and planters can help create an appealing streetscape depending upon their design and the current environment in which they are installed.

When placed, make sure that they accomplish their function and distance between them is appropriate. The distance must allow free flow of pedestrians, but restrict flow of vehicles.

Fragmentation is another concern with any barrier system, whether caused by bomb blast or vehicle impact.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

Unit IX-C-26

Barriers / Bollards /Fencing -- Jersey Barriers

Least desirable of barrier types
- Difficult to place and move
- No vehicle stopping capability unless tied to pavement with at least 4 pieces of #4 (1/2-inch diameter) rebar into pavement about 18 inches deep and/or tied together with steel cable (3/4 to 1-inch)
- Can cause sidewalk failure due to concentrated load and fact that sidewalk may be hollow underneath for storage or utilities
- Adds to fragmentation (barrier shatters) if vehicle bomb explodes next to barrier
- They impede access – pedestrians and first responders
  - Utilities (if placed on top of manholes)
  - Emergency access (fire trucks, ambulance, police)
  - ADA (Americans with Disabilities Act) access – crosswalks and ramps

Unit IX-C-27

Barriers / Bollards /Fencing -- Bollards

When placed, make sure that they accomplish their barrier function with an appropriate distance of not less than 4 feet-between them.

Bollards placed in long unbroken rows present a monotonous appearance and may appear as a wall from some angles.

<u>Pay attention</u> to how bollards or fences:
- Turn the corner
- Intersect with driveways and gates
- Cross pedestrian paths and handicapped ramps

In an urban environment, bollards and barriers are ideally the first layer of defense to obtain the most stand-off possible.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

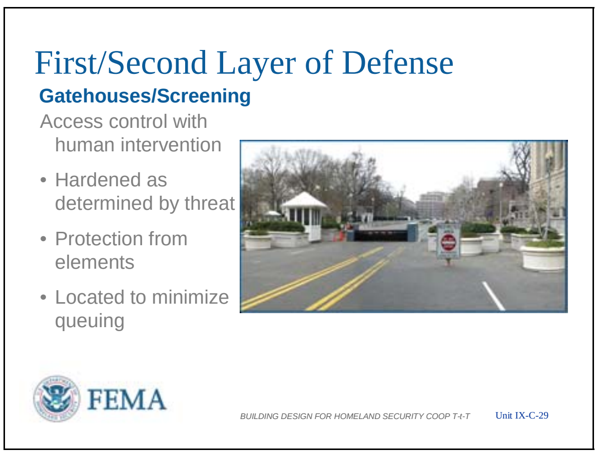
Unit IX-C-28

Barriers / Bollards /Fencing -- Fencing

Fencing can cover the range from being limited to channeling law-abiding people (pedestrians and vehicles) to being massive constructions with the intent of controlling malicious people and vehicles.

As a basic it provides access control for pedestrians and vehicles (usually with the help of other barriers). Fencing in each layer of defense is enhanced with electronic security – sensors and CCTV.

Unit IX-C-29



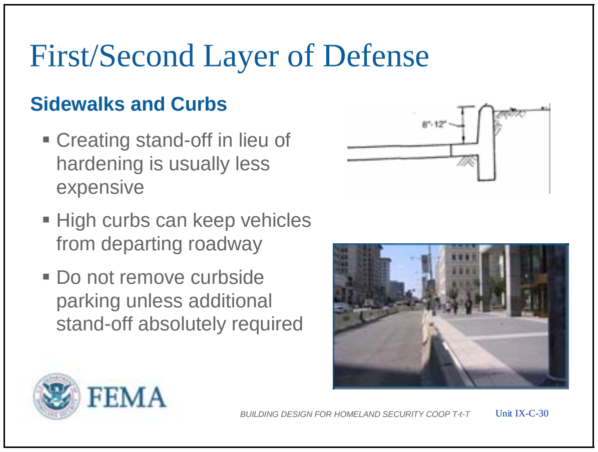
Gatehouses / Screening

Gatehouses are to assist the screening of vehicles and pedestrians to ensure they have proper authorization for access. This can be at the first layer of defense (normally) or at any restricted perimeter.

- Depending on the threat the gatehouse should be hardened, but at the very least PPE (personal protective equipment, like bullet-resistant vests) should be worn
- The elements – wind, rain, heat, cold make this job difficult enough that the gatehouse should provide a refuge with water, heat, and air conditioning, including a rest room
- Proper placement so that the guard can interact with drivers without having to cross the traffic lane and adequate throughput so that queues will not form waiting for access.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Unit IX-C-30



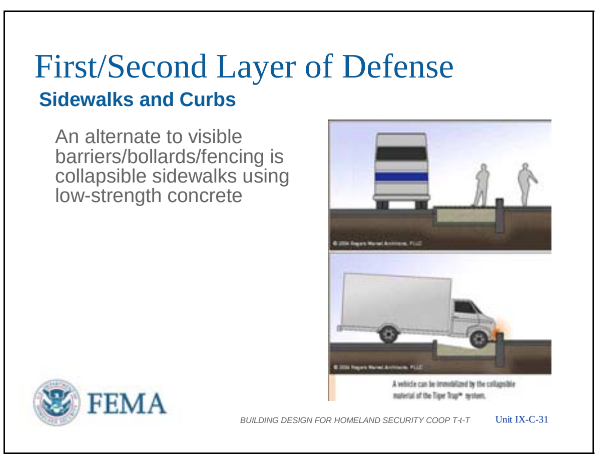
Sidewalks and Curbs

Sidewalks serve as the common space for pedestrian interaction, movements, and activity. Sidewalks should be open and accessible to pedestrians to the greatest extent possible and security elements should not interfere with circulation particularly in crowded locations

Curbside parking should not be removed unless additional stand-off distance is absolutely necessary for high-risk buildings. Prohibiting on street parking or closing lanes should only be used as a temporary measure during times of increased alert.

High curbs and other measures may be installed to keep vehicles from departing the roadway (especially if curb height is at the axle height, but ensure ADA requirements are met at intersections). In one instance, an armored car firm was asked to park their vehicles around a building that had received credible threats to act as barriers and increase stand-off.

Unit IX-C-31



Sidewalks and Curbs

Another unobtrusive approach for providing a vehicle barrier is combining collapsible sidewalk with a small wall that will catch a vehicle bumper. The sidewalk is made of low-strength concrete that takes pedestrian weight but not vehicle weight.

These graphics are of the Rock Twelve Security Architecture Tiger Trap ™ and their product literature information:

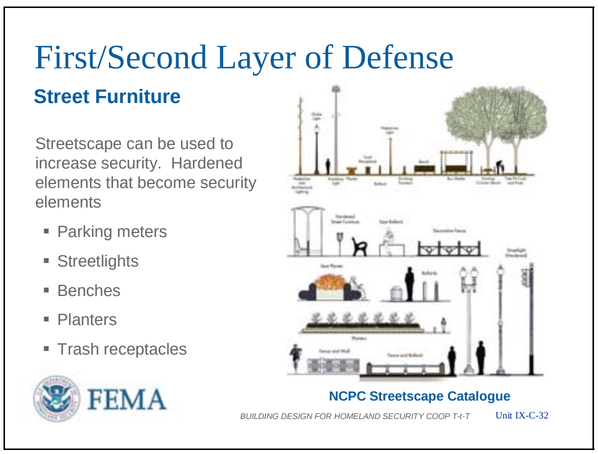
- Designed to reduce the impact of security on public space, this innovative vehicle arrest system utilizes a subgrade compressible material that lowers the elevation of an attacking vehicle and a

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

low wall that then halts the lowered vehicle.

- The subgrade compressible material allows the rear wall to be as low as a bench or even completely below grade.
- The compressible material combined with a decorative covering surface supports pedestrian loads, but fails under the weight of a vehicle.

Unit IX-C-32



Street Furniture

At the site perimeter, walls and fences may be hardened (strengthened) to resist the impact of a weapon-laden vehicle. However, planters, bollards or decorative boulders can accomplish the same objective in a much more aesthetically pleasing manner.

The streetscape can included hardened versions of parking meters, street lights, benches, planters and trash receptacles that act as barriers to moving vehicles.

The National Capital Planning Commission (NCPC) provides a catalog that shows several examples of hardened streetscape furniture.

Unit IX-C-33

Street Furniture

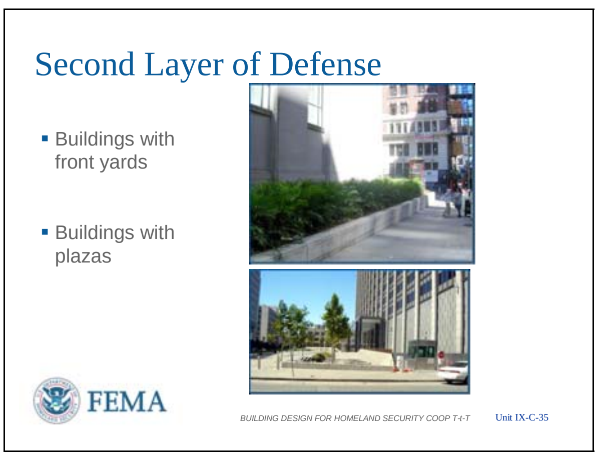
The scale of the streetscape should be appropriate to its primary users and it can be manipulated to increase the comfort level of desired users while creating a less inviting atmosphere for users with malicious intent.

It is critical to maintain important functions such as adequate space for pedestrian circulation and appropriate distances between vehicles and security barriers. The recommended distance to place streetscape security components is at least 24 inches from

INSTRUCTOR NOTES

Unit IX-C-34
Hidden Slide

Unit IX-C-35



CONTENT/ACTIVITY

the edge of the curb to allow for the opening of car doors and pedestrian movement from car to sidewalk.

Well planned barriers can also assist in clearly defining areas of public and private space and in protecting pedestrians from traffic.

Street Furniture

Numerous urban design elements present opportunities to provide security. Even at the pedestrian scale, certain operational requirements must be accommodated. For example, although efficient pedestrian and vehicle circulation systems are important for day-to-day living, they are also critical for emergency response, evacuation, and egress. Furthermore, despite an emphasis on downsizing the scale of the streetscape, it is critical to maintain the maximum stand-off distance possible between vehicles and structures.

Yards and Plazas

Three generic site types will be found in the central business district of any large city.

- Buildings with zero setback and alleys. The building face is on the property line. An alley is a narrow street that divides a city block and provides service access to the side or rear of the building.
- Buildings with front yards. The building is set back from its property line and the space is usually landscaped. The building yard includes pedestrian entries and loading docks.
- Building with plazas. The building is placed within an open space that is publicly accessible.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Unit IX-C-36

Building Yard

Some buildings have a “yard” between the building face and the sidewalk. The yard is within the property line and typically consists of a grassy or planted area adjacent to the building.

Yards are typical, narrow, of the order of 10 to 20 feet, providing some stand-off distance.

The yard may be flush or raised above the level of the sidewalk. A raised yard can provide a barrier to vehicles.

Major public buildings may have wide yards that are more of a landscaped forecourt that can offer reasonable stand-off distance. Yards are usually provided for governmental or institutional buildings in which coverage of the entire property may not be economically critical as is the case for private development.

Sometimes small yards (within the property line) are matched with a wide sidewalk provided by the city.

Unit IX-C-37

Building Yard

A typical raised, low planter that can act as a bench (or plinth wall that holds back soil or rock), as shown in the left photo, presents a significant barrier to small and medium-sized vehicles. The high stepped yard in the right photo, which is along the side of the building, is a significant barrier and could also act as a deflector of explosive blast from a curbside vehicle bomb.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

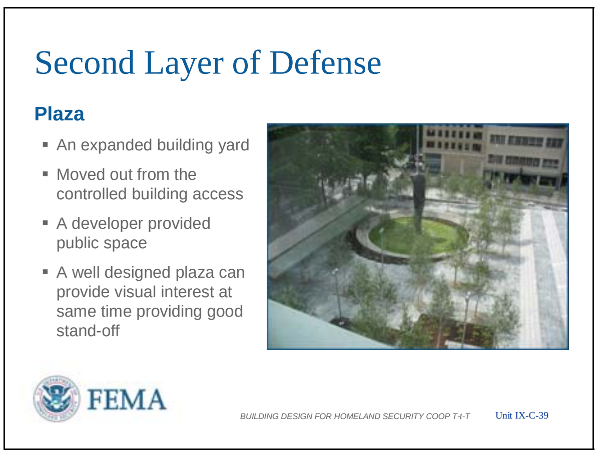
Unit IX-C-38

Building Yard

Security elements within the building yard should complement the building architecture and landscaping and should be designed so as to appear as well designed landscape objects rather than expressing security. The security elements should be located near the outer edge of the yard to maximize stand-off.

Good examples of this are shown in these photos.

Unit IX-C-39



Plaza

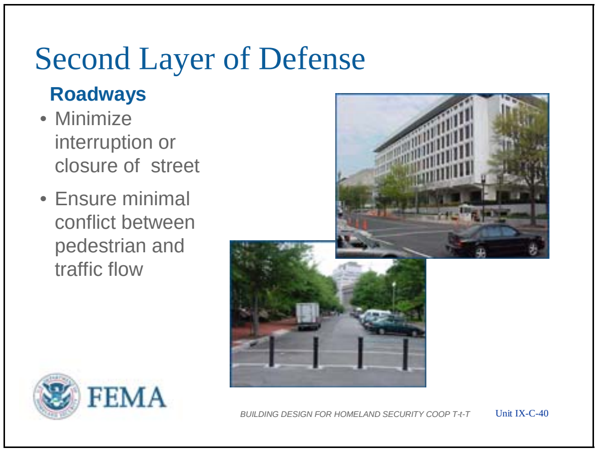
Extensive business district development with very large buildings began after World War II. The straight tower with no setbacks became fashionable, but new ordinances permitted building developers to construct taller buildings, with greater floor area, if a public plaza was incorporated. In fact, in Tokyo, new high-rises must ensure they do not completely block the sun from surrounding buildings.

In effect, the plaza became an expanded building yard. It was moved outside the controlled access space of the building and became public space provided by the developer.

The additional space provided by plazas enables a more effective second layer of defense to be achieved. Often an acceptable stand-off distance can be created on one or more faces of the building depending on the plaza /building layout.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Unit IX-C-40

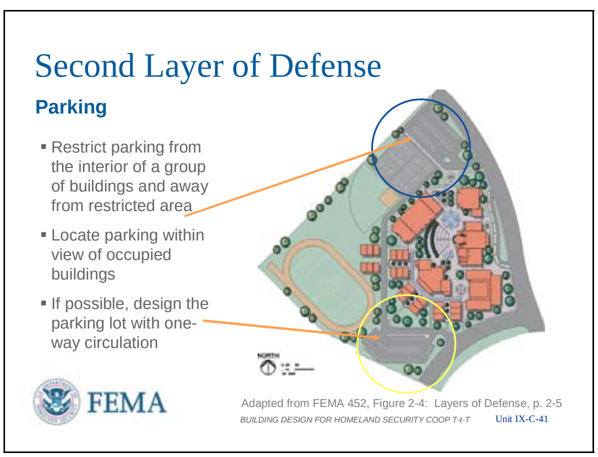


Roadways

Given that the energy transferred when one object strikes another is a function of its mass and its velocity, a bollard that can stop a 15,000-pound truck moving at 35 miles per hour may not be able to stop the same truck moving at 55 miles per hour. In developing a system of street alignments with protection in mind, the designer cannot determine the size or weight of a vehicle that will travel along the road. However, the designer can propose a roadway system to minimize vehicle velocity, thus using the roadway itself as a protective measure.

Minimizing street closure and disrupting vehicle and pedestrian patterns should always be a goal. But at higher threats, these measures may be among the few available mitigation options.

Unit IX-C-41



Parking

Building placement on the site must balance stand-off distances; relationship to adjacent streets and buildings; siting of utilities, parking areas, and driveways; as well as access to parking and loading areas.

There are three primary types of parking facilities, all of which present security trade-offs.

- Surface lots can be designed to keep vehicles away from buildings, but they consume large amounts of land and, if constructed of impervious materials, can contribute greatly to stormwater runoff volume. They can also be hazardous for pedestrians if dedicated pedestrian pathways are not provided.
- In contrast, street parking is often convenient for users and a source of revenue for local governments (parking meters), but

INSTRUCTOR NOTES	CONTENT/ACTIVITY

this type of parking may provide little or no setback.

- Finally, garage structures provide revenue and can be convenient for users, but they may require structural measures to ensure blast resistance as well as crime prevention measures to prevent street crime.

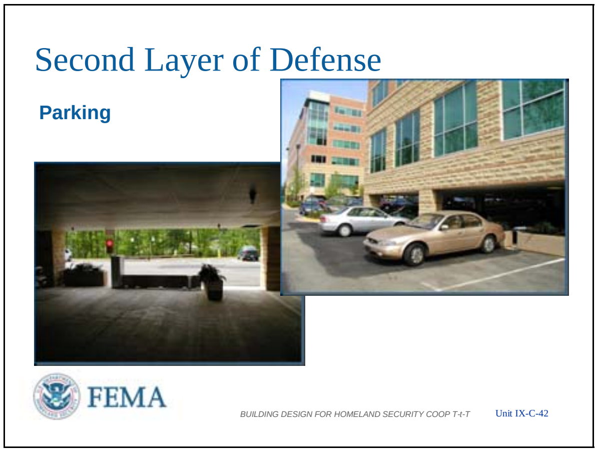
Although the cost of land suggests that the construction of a garage (either underground or aboveground) may be the most economically viable approach for many developments, they can be highly vulnerable to vehicle-borne weapons, endangering the building above in the most commonly found configuration. If garages must be used, human security procedures (e.g., vehicle searches) and electronic systems (e.g., closed circuit television) may be necessary.

Parking structures open to the public should be sited and evaluated with concern for stand-off from other buildings, screening from critical operations and sensitive areas that might be observed from within the parking structure, and as a point of access or staging for use of weapons or explosives. Progressive collapse can become a concern in parking structures.

If stand-off distance is needed between a building and a First Layer controlled perimeter, placing parking in this area is an excellent use of the available space, as shown in this graphic.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Unit IX-C-42

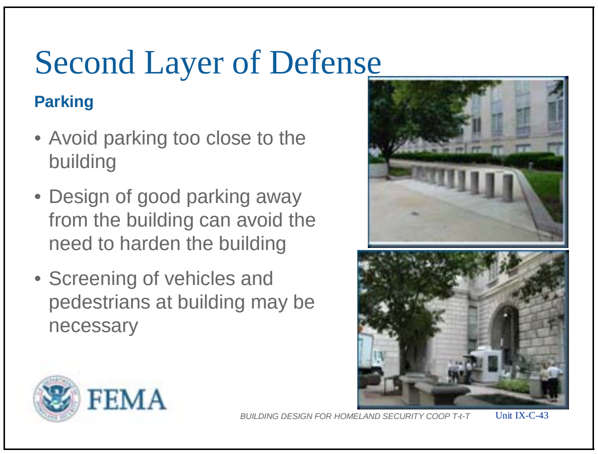


Parking

Parking layout and circulation is often one of the largest program elements in site design. Public street parking, parking lots, free standing structured parking buildings, and underground parking have different characteristics to be considered.

Note the limited physical barriers that are in place to prevent unauthorized vehicles from getting underneath this building as shown in the slide. Also note the limited stand-off and the parking proximity to columns supporting the exterior wall of the building.

Unit IX-C-43
Hidden Slide



Parking

Avoid parking too close to the building, especially large vehicles.

Good parking design can prevent the need to harden the building.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Unit IX-C-44

Second Layer of Defense

Parking

- Restrict parking and access between buildings
- Consider one-way circulation in parking lots
- Locate parking within view of occupied buildings
- Restrict parking underneath buildings
- Well-lit, with security presence, emergency communications, and/or CCTV
- Apply progressive collapse hardening to columns when parking garage is in the building

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IX-C-44

Parking

When designing parking, the following should be taken into consideration:

- Maintain stand-off distance from building
- Restrict parking from the interior of a group of buildings and away from any restricted area
- Avoid having parking near, within or underneath buildings – Consider hardening against progressive collapse if parking garage is in the building.
- Locate parking within view of occupied buildings
- If possible, design the parking lot with one-way circulation that restricts straight-on high-speed approaches to buildings
- Provide signage to clearly mark separate entrances for different parking lots
- Keep parking areas well lit; use emergency communications, and/or CCTV

Unit IX-C-45

Second Layer of Defense

Parking - Loading Docks

- Avoid trucks parking into or underneath of the buildings
- Keep dumpsters away from buildings
- Separate loading docks from building critical functions
- Design to prevent progressive collapse

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IX-C-45

Significant structural damage to the walls and ceiling of the loading dock may be acceptable; however, the areas adjacent to the loading dock should not experience severe structural damage or collapse.

Parking – Loading Docks

Loading docks and service access areas are commonly required for a building and are typically desired to be kept as invisible as possible.

- Locate loading docks so that vehicles will not be allowed underneath the building or too close to the building at the curb lane. If this is not possible, the dock area should be hardened for blast.
- Design to prevent progressive collapse, especially if loading dock is under the building.
- Separate (by at least 50 feet) loading docks and shipping and receiving areas in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems,

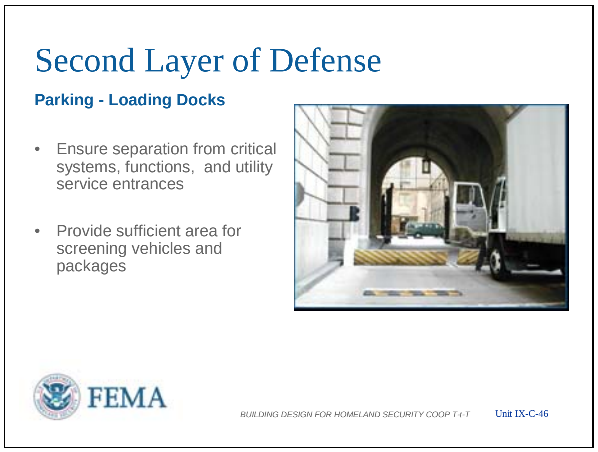
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

fire suppression water mains, cooling and heating mains, etc.

- Siting and layout of loading areas should be secured and accommodate sufficient area for screening vehicle and packages.
- Trash dumpsters should be relocated away from the building. (Explosive devices can be tossed in the dumpster creating a blast effect.)

This photo is a good example of a loading dock that is not underneath the building. This will be covered in more detail in the next instruction unit.

Unit IX-C-46

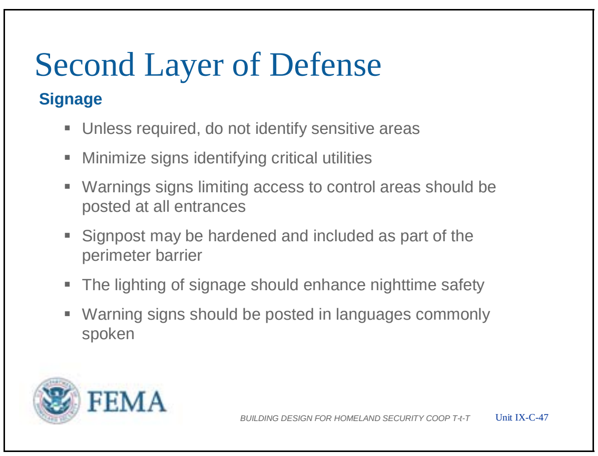


Parking – Loading Docks

Loading dock on-site accommodation is essential. Security issues relating to loading docks must be examined on a site by site basis, possibly involving the cooperation of civic authorities, especially in an urban environment.

For increased threat levels, you may coordinate local policy to screen vehicles before approaching the loading dock. In any case, the vehicles need an inspection area established for normal operations at lower threat levels in order to protect the building.

Unit IX-C-47



Whatever the strategy for signage, it is important that signage be developed in concert with other site design elements, be included in the site design palette, and

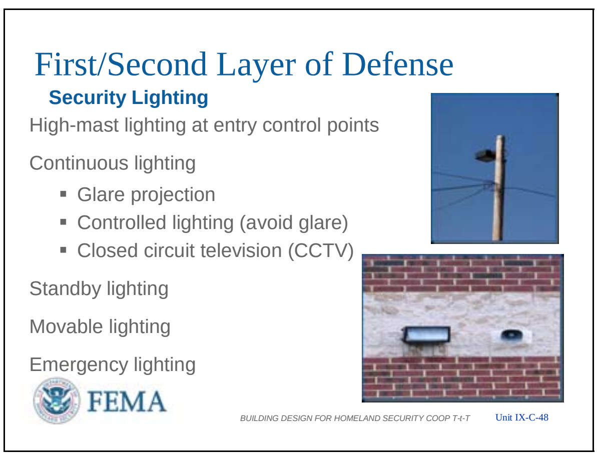
Signage

Building owners should determine how visible the project should be and corresponding implications for site signage. For some projects, a degree of anonymity may be part of the security strategy.

- Unless required, signs should not identify sensitive areas.
- Minimize signs identifying critical utility complexes, such as power plants and water treatment plants.
- Warning signs should be posted at all entrances to limited, controlled, and exclusion areas.
- The wording on the signs should denote warning of a restricted area.
- Signs should be posted at intervals of no

designed and placed in coordination with all other materials. To reduce the potential of clutter, signage should be integrated with other streetscape elements and architectural elements. Access, maintenance, and adaptability should be considered in selection of signage systems. Periodically changes are required to signage content. A comprehensive signage plan should be tailored to the mission of the facility accompanying the FEMA 426 guidelines.

Unit IX-C-48



more than 100 feet and should not be mounted on fences equipped with intrusion-detection equipment.
- Signage may be mounted on other elements, such as fences and walls to reduce the number of posts along the street or perimeter.
- Signposts may be hardened and included as part of the perimeter barrier.
- The lighting of signage may also enhance nighttime safety to those who come to the site during evening or early morning hours.
- Locate variable message signs, which give information on site/organization special events and visitors, so that they are not observable from site perimeters (first layer)
- Warning signs must use languages commonly spoken.

Security Lighting

Security lighting should be provided for overall site and building illumination and along the perimeter to allow security personnel to maintain visual assessment during darkness. Lighting is desirable around areas such as piers, fence lines, loading docks, storage areas, and parking lots. At entry points, a recommended minimum surface lighting average of 4 horizontal foot candles will help ensure adequate lighting.

Security lighting has different purposes – to blind, to allow vehicle inspection, to identify credentials, to support CCTV capabilities, etc. Thus, security lighting must be coordinated for all purposes.

INSTRUCTOR NOTES

Unit IX-C-49

Unit IX-C-50

A thorough walk-through of the site property should be conducted and proper protection devices should be applied to exposed utilities. The electrical substation shown can be easily damaged from outside the fenceline by projectiles or short circuiting actions. The structure on the right only has fencing on three sides.

CONTENT/ACTIVITY

Sensors / CCTV

Manned and electronic security increases deterrence and detection with attendant reduction in risk. It is the fastest technology to add and upgrade when selected, installed, and used properly.

It should cover vehicle, pedestrian, and utility entrances as all of these are potential approaches for terrorist tactics.

This will be covered in more detail under Electronic Security Systems later.

Site Utilities

Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion.

Loss of a utility because access was readily available to a potential threat element is one reason for assessing site utilities to ensure physical security measures are in place to limit access to authorized personnel only.

INSTRUCTOR NOTES

Unit IX-C-51

CONTENT/ACTIVITY

Site Utilities

- Top Right – Open Gate allowing access to Critical Cooling Unit for Computer Center
- Lower Right – Exposed air conditioning systems
- Middle – antenna system for Emergency Operations Center accessible from the ground
- Lower Left – Exposed generator and natural gas regulators

Concealed or underground utilities are easier to protect than exposed or aboveground constructions.

Access to utilities should be protected or secure, allowing only authorized personnel access to perform maintenance and repair.

If physical security measures cannot limit access, then add sensors/CCTV to provide added protection.

The location and accessibility of site utilities directly impacts the vulnerability of systems to disruption and failure.

Incoming utility systems should have two entry points to the site for redundancy as required by criticality.

Looped versus radial distribution of utilities on site allows for higher system reliability and faster repair by avoiding utility loss by a single incident.

When selecting locations for utilities, be aware of possible conflicts and spacing requirements both horizontally and vertically. In addition there can be demand for underground zones for planting beds and foundations for hardened street furniture.

INSTRUCTOR NOTES

Unit IX-C-52
Hidden Slide

Unit IX-C-53
Hidden Slide

CONTENT/ACTIVITY

Site Utilities

The U.S. utility infrastructure is highly concentrated, utilizing the same rights-of-way, tunnels, underground conduits, and other service points. Examine where the utilities intersect (manholes, poles, city blocks, etc.) to find critical nodes.

Even if the utility is underground, manholes that provide access to the system should be physically secured.

Install fencing and if possible, remote monitoring capability at key electrical substations, pumping plants, and communications vaults.

Best Practices

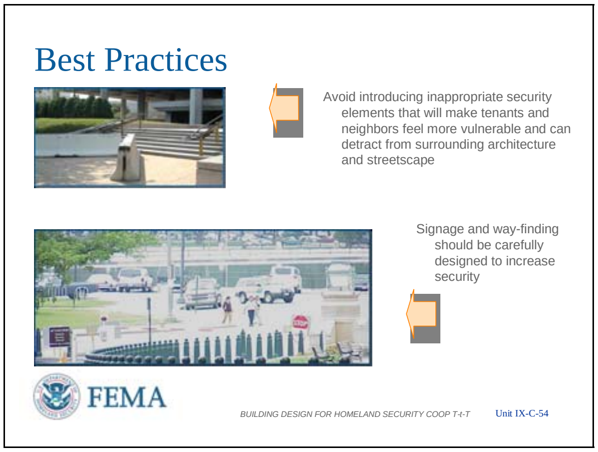
Best practices include but are not restricted to the following:

- Appropriate design can blend security into the existing streetscape and serve as amenities for tenants and neighbors
- Treatment of the security elements should be compatible existing elements – so that they do not look like security elements
- Perimeter barriers can be hand-in-hand with streetscape improvements and street planting
- Careful design attention should be paid to how bollards or fences turn the corner, intersect with driveways and gates, cross pedestrian paths and handicapped ramps
- Avoid street closure and removal of parking as the only solution of establishing stand-off distance
- Landscaping can provide visual interest and at the same time provide good stand-off

INSTRUCTOR NOTES

CONTENT/ACTIVITY

Unit IX-C-54
Hidden Slide

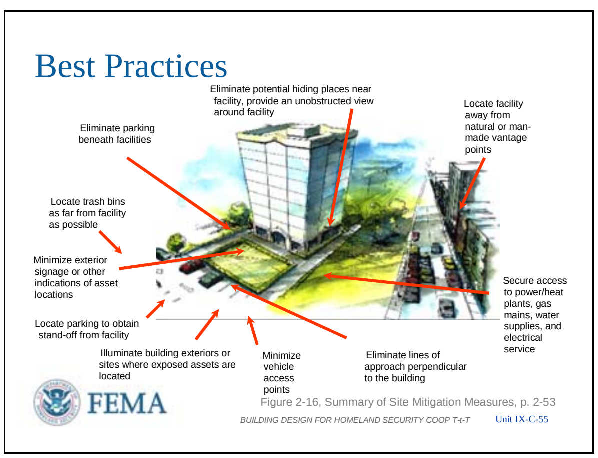


Best Practices

Good examples to follow and bad examples to avoid:

- Avoid introducing inappropriate security elements that will make tenants and neighbors feel more vulnerable and can detract from surrounding architecture and streetscape – jersey barrier at entrance steps – also ineffective as placed directly on pavement
- Signage and way-finding should be carefully designed to increase security
- Long expanses of bollards should be carefully designed and sited to avoid monotony – as can be seen in the lower photo
- Use perimeter barriers to define pedestrian zones and increase the safety of pedestrian by separating them from vehicular traffic
- Avoid designing perimeter barriers that impair access by first responders

Unit IX-C-55



Page 2-52 of FEMA 426 provides a comprehensive list of security/protection measures that can be taken – increasing in *protection, cost, and level of effort* – that

Best Practices

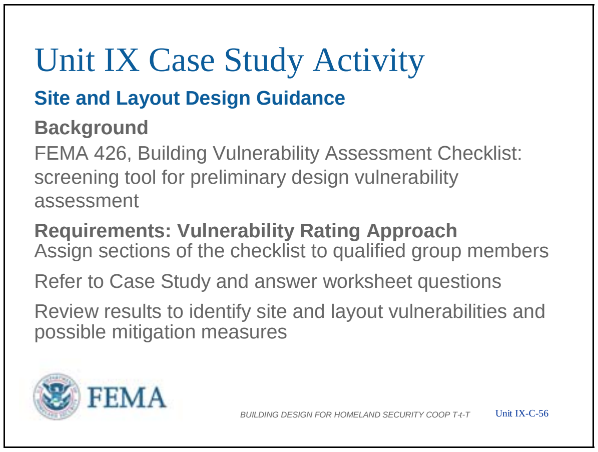
To summarize:

- A broad spectrum of mitigation actions can be taken – with a wide range of cost, protection provided, and level of effort required by the asset owner.
- The nominal ranking of mitigation measures on Page 2-52 provides a framework for the identification of short-term and long-term measures that can be taken.
- This is a great summary slide and can be found in FEMA 426 and the Air Force Installation Force Protection Guide on your Student Reference CD.

INSTRUCTOR NOTES

complements this graphic on Site Mitigation Measures.

Unit IX-C-56



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

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

There are <u>29 questions</u> to answer by the team and then confer. With an average of 7 team members this means each member answers about 4 questions or about <u>7 minutes per question</u> during their 30 minutes of research.

CONTENT/ACTIVITY

Student Activity

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

Activity Requirements

- Continue working in your small groups.
- Assign sections of the checklist to the group member who is most knowledgeable and qualified to perform an assessment of the assigned area.
- Refer to the Case Study to determine answers to the worksheet questions.
- Then review results to identify vulnerabilities and possible mitigation measures.

Take 45 minutes to complete this activity broken down as 30 minutes of research and 15 minutes of group interaction to compare information and discuss mitigation measures. Solutions will be reviewed in plenary group, taking about 15 minutes to ensure no group is drastically off track.

Transition

Unit IX covered the First and Second Layers of Defense.

Unit X will cover Building Design Guidance which includes the Third Layer of Defense.

UNIT IX (C) CASE STUDY ACTIVITY:
SITE AND LAYOUT DESIGN GUIDANCE
(COOP Version)

In this student activity, the emphasis is identifying vulnerabilities in the site and layout design. The **Building Vulnerability Assessment Checklist in FEMA 426 (Table 1-22, pages 1-46 to 1-93)** provides a tool for vulnerability assessment of the proposed and existing sites and buildings.

Requirements

Assign sections of the checklist to group members who are most knowledgeable and qualified to perform an assessment of the assigned area. Refer to the Appendix C Case Study to determine answers to the questions. Then review results as a team to identify vulnerabilities and possible mitigation measures.

Activity # 1: Complete the selected vulnerability checklist questions in the following Vulnerability Questions table.

> **Note**: There are **29** questions below (**13** in Section 1, **5** in Section 2, and **11** in Section 5), so it is recommended that the team split up the questions among themselves taking 3-5 questions each and review the Appendix C Case Study for answers. Apportion the available time for gathering the answers and then provide each other the answers while performing the actions below.

Activity # 2: Upon completion of the questions refer back to the vulnerability ratings determined in the Unit IV (C) Student Activity. Based on this more detailed analysis, decide if any vulnerability rating needs adjustment. Adjust the Risk Matrix poster accordingly for any changes in vulnerability rating.

Activity # 3: Select mitigation measures to reduce vulnerability and associated risk from the site and layout perspective. Concentrate on the three highest risk ratings on the Risk Matrix poster as adjusted by Activity # 2. Use the Site and Layout Design Mitigation Measures table found at the end of this unit to capture this information.

Activity # 4: Consider the mitigation measures of Activity #3 to be installed, estimate the new vulnerability ratings as if these measures were in place, and calculate the new risk ratings. Capture your information in the Site and Layout Design Mitigation Measures table.

Section	Vulnerability Question	Guidance	Observations
1	**Site**		
1.1	What major structures surround the facility (site or building(s))?	**Critical infrastructure to consider includes:** **Telecommunications infrastructure** Facilities for broadcast TV, cable	***There are two large manufacturing plants with large quantities of hazardous materials stored on site within 2 miles of the***

Section	Vulnerability Question	Guidance	Observations
	What critical infrastructure, government, military, or recreation facilities are in the local area that impact transportation, utilities, and collateral damage (attack at this facility impacting the other major structures or attack on the major structures impacting this facility)?	TV; cellular networks; newspaper offices, production, and distribution; radio stations; satellite base stations; telephone trunking and switching stations, including critical cable routes and major rights-of-way **Electric power systems** Power plants, especially nuclear facilities; transmission and distribution system components; fuel distribution, delivery, and storage **Gas and oil facilities** Hazardous material facilities, oil/gas pipelines, and storage facilities **Banking and finance institutions** Financial institutions (banks, credit unions) and the business district; note schedule business/financial district may follow; armored car services **Transportation networks** Airports: carriers, flight paths, and airport layout; location of air traffic control towers, runways, passenger terminals, and parking areas Bus Stations Pipelines: oil; gas Trains/Subways: rails and lines, railheads/rail yards, interchanges, tunnels, and cargo/passenger terminals; note hazardous material transported Traffic: interstate highways/roads/tunnels/ bridges carrying large volumes; points of congestion; note time of day and day of week Trucking: hazardous materials cargo loading/unloading facilities; truck terminals, weigh stations, and rest areas Waterways: dams; levees; berths and ports for cruise ships, ferries, roll-on/roll-off cargo vessels, and container ships; international (foreign) flagged vessels (and cargo) **Water supply systems** Pipelines and process/treatment facilities, dams for water	***CI/BC building, one to the north and the other to the southwest. In addition, there are more than a dozen Tier II HazMat facilities within 3 miles of the building (in all directions).*** ***A major interstate highway is located within ¼ mile of CI/BC.*** ***CSX Transportation and Norfolk-Southern Railway maintain a transportation corridor about ½ mile from CI/BC. There appears to be no restrictions on the material carried along these rail lines.*** ***A leg of the Piedmont Petroleum Pipeline (PPP) runs underneath the office park in the vicinity of CI/BC. Part of Piedmont's regional network, this portion of the pipeline normally carries a variety of refined products, including commercial and military jet fuels, diesel and three grades of gasoline, home heating fuels, etc. Four buried pipes carry approximately 20 million gallons per day.*** ***Connected to the pipeline, less than 1 mile from CI/BC, is a 20-million gallon capacity fuel farm. Operated by the Shellexxico Company, this tank farm stores a variety of petroleum products, primarily gasoline.*** ***Two airports are in the vicinity of CI/BC. One is a major international airport approximately 8 miles away. The other is a small, but busy general aviation***

Section	Vulnerability Question	Guidance	Observations
		collection; wastewater treatment **Government services** Federal/state/local government offices – post offices, law enforcement stations, fire/rescue, town/city hall, local mayor's/governor's residences, judicial offices and courts, military installations (include type-active, Reserves, National Guard) **Emergency services** Backup facilities, communications centers, Emergency Operations Centers (EOCs), fire/Emergency Medical Service (EMS) facilities, Emergency Medical Centers (EMCs), law enforcement facilities **The following are not critical infrastructure, but have collateral damage potential to consider:** **Agricultural facilities:** chemical distribution, storage, and application sites; crop spraying services; farms and ranches; food processing, storage, and distribution facilities **Commercial/manufacturing/industrial facilities:** apartment buildings; business/corporate centers; chemical plants (especially those with Section 302 Extremely Hazardous Substances); factories; fuel production, distribution, and storage facilities; hotels and convention centers; industrial plants; raw material production, distribution, and storage facilities; research facilities and laboratories; shipping, warehousing, transfer, and logistical centers **Events and attractions:** festivals and celebrations; open-air markets; parades; rallies, demonstrations, and marches; religious services; scenic tours; theme parks **Health care system components:** family planning clinics; health	***airport approximately 2 miles away.***

Section	Vulnerability Question	Guidance	Observations
		department offices; hospitals; radiological material and medical waste transportation, storage, and disposal; research facilities and laboratories, walk-in clinics **Political or symbolically significant sites:** embassies, consulates, landmarks, monuments, political party and special interest groups offices, religious sites **Public/private institutions:** academic institutions, cultural centers, libraries, museums, research facilities and laboratories, schools **Recreation facilities**: auditoriums, casinos, concert halls and pavilions, parks, restaurants and clubs (frequented by potential target populations), sports arenas, stadiums, theaters, malls, and special interest group facilities; note congestion dates and times for shopping centers References: *FEMA 386-7, FEMA SLG 101, DOJ NCJ181200*	

Section	Vulnerability Question	Guidance	Observations
1.2	Does the terrain place the building in a depression or low area?	Depressions or low areas can trap heavy vapors, inhibit natural decontamination by prevailing winds, and reduce the effectiveness of in-place sheltering. Reference: *USAF Installation Force Protection Guide*	***Based on terrain elevation data, the ground level of the tank farm is 49 feet higher than the ground level at CI/BC. Only some of the fuel tanks are bermed, but leaking fuel is not likely to reach CI/BC's office park. The interstate highway between the two is 16 feet lower than the tank farm and slightly lower than the office park. Thus, any leak will follow the interstate and not reach CI/BC.*** ***The rear parking area behind CI/BC slopes steeply away from the building to a stream which allows winds to pass over the structure unhindered.*** ***CI/BC is not in a depression or low area.***
1.4	Is a perimeter fence or other types of barrier controls in place?	The intent is to channel pedestrian traffic onto a site with multiple buildings through known access control points. For a single building, the intent is to have a single visitor entrance. Reference: *GSA PBS-P100*	***There is no fence or other type of barrier on the site's perimeter. The only fence is a short 4-foot high fence for life safety to keep anyone from falling down the steep embankment in the rear of the building.***
1.5	What are the site access points to the site or building?	The goal is to have at least two access points – one for passenger vehicles and one for delivery trucks due to the different procedures needed for each. Having two access points also helps if one of the access points becomes unusable, then traffic can be routed through the other access point. Reference: *USAF Installation Force Protection Guide*	***There are three vehicle access points into the parking lot spread along the main road.*** ***Access to the CI/BC building includes the loading dock on the west side (rear) of the building and front entrance with an 8-foot overhang.*** ***There are three exits from the mezzanine and four exits from the building.***

Section	Vulnerability Question	Guidance	Observations
1.7	Is there vehicle and pedestrian access control at the perimeter of the site?	Vehicle and pedestrian access control and inspection should occur as far from facilities as possible (preferably at the site perimeter) with the ability to regulate the flow of people and vehicles one at a time. Control on-site parking with identification checks, security personnel, and access control systems. Reference: *FEMA 386-7*	***There is no access control to the site; however, security personnel monitor parking areas, and rear parking areas are well lit and monitored by CCTV cameras. Front parking areas are lit only.*** ***Proximity card readers prevent access to CI/BC by unauthorized personnel for normal entry, i.e. not criminal entry through forced entry means.***
1.10	What are the existing types of vehicle anti-ram devices for the site or building? Are these devices at the property boundary or at the building?	Passive barriers include bollards, walls, hardened fences (steel cable interlaced), trenches, ponds/basins, concrete planters, street furniture, plantings, trees, sculptures, and fountains. Active barriers include pop-up bollards, swing arm gates, and rotating plates and drums, etc.	***There are no vehicle anti-ram barriers installed, either at the property boundary or at the building.***
1.13	Does site circulation prevent high-speed approaches by vehicles?	The intent is to use site circulation to minimize vehicle speeds and eliminate direct approaches to structures. Reference: *GSA PBS-P100*	***No, entering at the center access point from the main road, turning left, and then turning right to proceed in front of the southern-most building, a car could easily reach 75 mph when striking the CI/BC building. The other two approaches have 90-degree turns at the end which severely hampers high-speed approach to CI/BC.***
1.14	Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?	Single or double 90-degree turns effectively reduce vehicle approach speed. Reference: *GSA PBS-P100*	***There are three long straightaways approaching the CI/BC building, with only one that is straight enough to achieve a high speed approach. Thus, turns on the two northernmost approaches have benefit in reducing vehicle approach speed toward the CI/BC building.*** ***Using speed bumps,***

Section	Vulnerability Question	Guidance	Observations
			especially angled speed bumps would be one way to reduce speed. Using barriers to direct traffic so there is no long straightaway is another approach. An "S" route entrance may be frustrating for visitors, but would significantly reduce the maximum speed capability of any vehicle approach to the buildings. ***As a minimum, closing off the parking slots serving the central building in the complex (the one CI/BC is in) with barriers or planters should be considered as a minimum to reduce high speed approach and increase stand-off. Similarly, the tenants of the other two buildings may want the same correction to their buildings but with a major reduction in available parking spaces.***
1.16	Does adjacent surface parking on site maintain a minimum stand-off distance?	The specific stand-off distance needed is based upon the design basis threat bomb size and the building construction. For initial screening, consider using 25 meters (82 feet) as a minimum with more distance needed for unreinforced masonry or wooden walls. Reference: *GSA PBS-P100*	***Adjacent parking is that parking associated with the next building or site that is not under the control of the owners of the building being assessed.*** ***There is no adjacent parking per se as it is one office park, but the one parking lot or area can be used by any tenant or visitor to the office park. Stand-off distance to the front parking lot is less than the 82 feet screening value. Cars or trucks can drive up to the loading dock in the rear.***

Section	Vulnerability Question	Guidance	Observations
1.19	Do site landscaping and street furniture provide hiding places?	Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages. If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages. Reference: *GSA PBS-P100*	***There is no street furniture shown for this building.*** ***The landscaping shown is grass and trees are mature/tall enough so that a package cannot be hidden at the base. The hedge along the building drip line may conceal a package, if allowed to get taller or denser.*** ***There is no mail or express box and there is no slot in the glass main entrance door.*** ***Due to the size of the building columns, a package could be overlooked.***
1.20	Is the site lighting adequate from a security perspective in roadway access and parking areas?	Security protection can be successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, is critical. Illuminating Engineering Society of North America (IESNA) guidelines can be used. The site lighting should be coordinated with the CCTV system. Reference: *GSA PBS-P100*	***Both rear and front parking areas are well lit. Rear areas are also monitored by CCTV cameras.***
1.21	Are line-of-sight perspectives from outside the secured boundary to the building and on the property along pedestrian and vehicle routes integrated with landscaping and green space?	The goal is to prevent the observation of critical assets by persons outside the secure boundary of the site. For individual buildings in an urban environment, this could mean appropriate window treatments or no windows for portions of the building. Once on the site, the concern is to ensure observation by a general workforce aware of any pedestrians and vehicles outside normal circulation routes or attempting to approach the building unobserved.	***No, lines of sight are not integrated with landscaping and green space. There are clear, approximately 300-foot, lines of sight in all directions from buildings in this office park to easily accessible locations outside the office park.***

Section	Vulnerability Question	Guidance	Observations
		Reference: *USAF Installation Force Protection Guide*	
1.23	Are all existing fire hydrants on the site accessible?	Just as vehicle access points to the site must be able to transit emergency vehicles, so too must the emergency vehicles have access to the buildings and, in the case of fire trucks, the fire hydrants. Thus, security considerations must accommodate emergency response requirements. Reference: *GSA PBS-P100*	***Yes, fire hydrants in the office park are currently accessible and the hydrant nearest to CI/BC is 200 feet away.***
2	**Architectural**		
2.2	Is it a mixed-tenant building?	Separate high-risk tenants from low-risk tenants and from publicly accessible areas. Mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures. Reference: *GSA PBS-P100*	***The building is a multiple-tenant facility and there are multiple buildings in the office park with multiple tenants.*** ***CI/BC has neighbors on one side in its building and a different neighbor in the adjacent building.***
2.3	Are pedestrian paths planned to concentrate activity to aid in detection?	Site planning and landscape design can provide natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities. Also, prevent pedestrian access to parking areas other than via established entrances. Reference: *GSA PBS-P100*	***Each tenant facility has its own entrance, spreading pedestrian activity across the front of the buildings within easy observation of each entrance to aid in detection.*** ***Loading docks are likewise spread out across the rear of the buildings. CI/BC uses a CCTV camera on the building rear to aid in detection of personnel approaching the rear entrance.***
2.4	Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	The size of the trash receptacles and mailbox openings should be restricted to prohibit insertion of packages. Street furniture, such as newspaper vending machines, should be kept sufficient distance (10 meters or 33 feet) from the building, or brought inside to a	***There is no indication that there are trash receptacles and mailboxes in close proximity to the building.*** ***The dumpster is approximately 50 feet from the rear of the building.***

Section	Vulnerability Question	Guidance	Observations
		secure area. References: *USAF Installation Force Protection Guide and DoD UCF 4-010-01*	
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: Emergency generator, including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; Uninterruptible power supply (UPS) systems controlling critical functions; Main refrigeration and ventilation systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. Reference: *GSA PBS-100*	***This building is not large enough to maintain separation distances.*** ***Attack from the front of the building would primarily impact the Business Center and office space. Attack from the rear would affect critical utilities and, through the loading dock area, the heart of the company – the computer center.*** ***No critical components are hardened as seen by the natural gas and electric service to the building.*** ***The UPS, mechanical and electrical room, and the diesel generator could be affected by a single bomb less than 50 feet from all these areas or taken out by a single wayward truck.***
2.16	Are high value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building. Reference: *GSA PBS-100*	***People are located along the exterior wall at the front of the building.*** ***The Information Division secure space and the Business Center secure offices have the best***

Section	Vulnerability Question	Guidance	Observations
			interior space location – not on an exterior wall, as does the main conference room. ***The Business Center is separated from the Information Division by a single wall, with secure spaces properly protected.*** ***Even though the Business Center is open to the public, access of the public comes under some controls within the building envelope.***
5	**Utility Systems**		
5.1	What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank) Is there a secure alternate drinking water supply?	Domestic water is critical for continued building operation. Although bottled water can satisfy requirements for drinking water and minimal sanitation, domestic water meets many other needs – flushing toilets, building heating and cooling system operation, cooling of emergency generators, humidification, etc. Reference: *FEMA 386-7*	***The water to the fire protection system within the building and the fire hydrants in the office park comes from the local municipal distribution mains which is also the source for all water uses in the building – rest rooms, kitchen/break room, HVAC equipment, etc. There is only one water supply line to the CI/BC building.*** ***Per request from employees, four bottled water dispensers are throughout the building, with an average of 2 water bottles (5 gallons each) in reserve at any given time for each dispenser.***
5.4	Does the building or site have storage capacity for domestic water? How many gallons of storage capacity are available and how long will it allow operations to continue?	Operational facilities will require reliance on adequate domestic water supply. Storage capacity can meet short-term needs and use water trucks to replenish for extended outages. Reference: *Physical Security Assessment for Department of Veterans Affairs Facilities.*	***The building currently stores drinking water as delivered in 5-gallon bottles. The site has the capacity to have 80 gallons on hand at the time of delivery. The bottled water supply would last for a few days to one week for drinking purposes only.*** ***There are no storage tanks for servicing other water***

Section	Vulnerability Question	Guidance	Observations
			uses in the CI/BC building.
5.5	What is the source of water for the fire suppression system? (local utility company lines, storage tanks with utility company backup, lake, or river) Are there alternate water supplies for fire suppression?	The fire suppression system water may be supplied from the domestic water or it may have a separate source, separate storage, or nonpotable alternate sources. For a site with multiple buildings, the concern is that the supply should be adequate to fight the worst case situation according to the fire codes. Recent major construction may change that requirement. Reference: *FEMA 386-7*	***The only water source for fire suppression is the municipal water mains serving the office park.***
5.10	What fuel supplies do the building rely upon for critical operation?	Typically, natural gas, propane, or fuel oil is required for continued operation. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***Heating for the CI/BC building is provided by a combination of natural gas and electricity.*** ***The backup electric generator uses diesel fuel.***
5.11	How much fuel is stored on the site or at the building and how long can this quantity support critical operations? How is it stored? How is it secured?	Fuel storage protection is essential for continued operation. Main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals). References: *GSA PBS-P100 and Physical Security Assessment for the Department of Veterans Affairs Facilities*	***Emergency power is provided by a single diesel generator, located in a shed in the rear parking lot. The generator has a 50-gallon day tank, maintained at 80 percent capacity. A 2,000-gallon main tank is buried under the parking lot, near the generator.*** ***There are no security measures for the fuel.***
5.12	Where is the fuel supply obtained? How is it delivered?	The supply of fuel is dependent on the reliability of the supplier. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***Natural gas enters the building through two meters under the loading dock staircase and is supplied from the local gas distribution company.*** ***Diesel fuel is delivered by truck from a local supplier, who normally responds the day after being called.***

Section	Vulnerability Question	Guidance	Observations
5.14	What is the normal source of electrical service for the site or building?	Utilities are the general source unless co-generation or a private energy provider is available. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***Electric power for CI/BC is provided by Hazardville Electric Company through two transformers outside the building. Two sets of buried transmission lines deliver 12,470 volt (12.47KV) power to the two separate transformers outside the building from a nearby substation.***
5.15	Is there a redundant electrical service source? Can the site or buildings be fed from more than one utility substation?	The utility may have only one source of power from a single substation. There may be only single feeders from the main substation. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***Each transformer with its respective feeder can handle the complete electrical load of CI/BC.*** ***However, both feeders come from the same substation.***
5.18	What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested? Is the emergency power collocated with the commercial electric service? Is there an exterior connection for emergency power?	Besides installed generators to supply emergency power, portable generators or rental generators available under emergency contract can be quickly connected to a building with an exterior quick disconnect already installed. Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability. Reference: *GSA PBS-P100*	***Emergency power is provided by a single diesel generator with a maximum capacity of 1250 KW/1562.5 KVA. This generator is large enough to take the complete load of the building.*** ***The backup diesel generator has never had to support CI/BC's power demands for longer than about 2 hours, and never with more than one chiller operating. It has never been tested for an extended period under a heavy load. The diesel generator is configured to automatically start upon loss of commercial power to the Computer Center Bus (CCB). This happens about twice a year due to electrical storms or utility maintenance in the neighborhood.*** ***Batteries to support the UPS were tested 2 years ago and calculated to provide 60***

Section	Vulnerability Question	Guidance	Observations
			minutes of power for orderly shutdown of the Computer Center. ***Using 0.08 gallons per hour per KW (a DoD design minimum) the generator with a 250 gallon day tank (80% full) and a 2,000 gallon storage tank will carry the maximum load for 22 hours, which would require daily refilling for an extended outage.*** ***The generator is outside the CI/BC building, but the Automatic Transfer Switch and commercial power service entrances are collocated in the Mechanical and Electrical Room.*** ***There is no exterior connection for electric power (like a fire pumper Siamese connection). A backup generator to the backup would either have to be wired to the Automatic Transfer Switch or spliced into the cables leaving the installed generator.***

Section	Vulnerability Question	Guidance	Observations
5.19	By what means do the main telephone and data communications interface the site or building?	Typically communication ducts or other conduits are available. Overhead service is more identifiable and vulnerable. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***CI/BC has two T1 lines and one T3 line connected at the demark to ATT's high performance backbone network. The ATT fiber connectivity provides more than enough bandwidth for CI/BC's current needs and planned future expansion.*** ***The demark is in the Comm Center on the opposite side of the building from the Mechanical and Electrical Room.*** ***As with all other utilities, the telephone and data service is underground.***
5.21	Does the fire alarm system require communication with external sources? By what method is the alarm signal sent to the responding agency: telephone, radio, etc.? Is there an intermediary alarm monitoring center?	Typically, the local fire department responds to an alarm that sounds at the station or is transmitted over phone lines by an auto dialer. An intermediary control center for fire, security, and/or building system alarms may receive the initial notification at an on-site or off-site location. This center may then determine the necessary response and inform the responding agency. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***The Security Officer has a key to the building that has the main fire panel. The main fire panel is located in the lobby area, which is open to unrestricted access during normal business hours. In the event of a fire, the panel alerts the local fire department and the security company using dedicated telephone lines.*** ***There is no intermediary alarm monitoring center, but the security company acts as a backup to ensure the fire department is alerted.***

Site and Layout Design Mitigation Measures
(COOP Version)

NOTE: There is too much variance in student answers compared to a "school solution" to populate this table with information that can be compared to the various team answers.

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

This page intentionally left blank

Unit X (C)

COURSE TITLE

Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer

TIME 165 minutes

UNIT TITLE

Building Design Guidance

OBJECTIVES

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

SCOPE

The following topics will be covered in this unit:

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

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-1 to 3-46 and 3-48 to 3-52; Checklist at end of Chapter 1
2. FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*
3. FEMA 430, *Site and Urban Design for Security*
4. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 5-1 to 5-16
5. FEMA 453, *Design Guidance for Shelters and Safe Rooms*
6. Case Study – Appendix C: COOP, Cooperville Information / Business Center
7. Student Manual, Unit X (C) (info only – not listed in SM)
8. Unit X (C) visuals (info only – not listed 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 Guides, Unit X (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit X (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers (one per team)

UNIT X (C) OUTLINE

8.	Fire Alarm Systems	1.5 minutes	IG-X-C-49
9.	Communications – Information Technology Systems	3 minutes	IG-X-C-50
10.	Equipment Operations and Maintenance	3 minutes	IG-X-C-52
11.	Security Systems	4.5 minutes	IG-X-C-54
12.	Practical Applications	1.5 minutes	IG-X-C-58
13.	Building Materials: General Guidance	1.5 minutes	IG-X-C-58
14.	Desired Building Protection Level	1.5 minutes	IG-X-C-59
15.	Summary/Activity/Transition	3.0 minutes	IG-X-C-60
16.	Student Activity: Building Design Guidance (Version **(C) COOP**) [45 minutes for students, 15 minutes for review]	60 minutes	IG X-C-62

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** This is a generic instruction unit, but it has great capability for linking to the Local Area. Local Area discussion may be generated as students have specific situations for which they would like to determine vulnerabilities or vulnerability rating prompted by points brought up in the presentation.

- **Optional Activity:** There are no optional activities in this unit. However if the Group Roundtable / Plenary / Discussion session is held after Unit IX, then the student activities for Units IX and X will be accomplished after the Unit X presentation.

- **Activity:** The students will continue familiarizing themselves with the Case Study materials. The Case Study is a risk assessment and analysis of mitigation options and strategies for an alternate facility to be assessed for potential Continuity of Operations (COOP). This alternate facility is a typical commercial office building located in a suburban business park. The assessment uses the DoD Antiterrorism Standards and the GSA Interagency Security Criteria to determine Levels of Protection and identify specific vulnerabilities. Mitigation options and strategies will use the concepts provided in **FEMA 426** and other reference materials.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page (Unit #) in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- "Walk through" the pages of the activity with the students, describing the steps followed to obtain the answers in the completed examples, and what is expected of the groups for this activity.
- For this activity, the assessment of the site and layout of the building in greater depth may result in the group adjusting the Risk Matrix scores for vulnerability rating, with resultant changes to risk rating. Transfer these changes 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 checklist section of questions, in summary fashion or select representative questions in each section as the starting points of discussion. 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. Note, there are no right or wrong answers, but all answers must be justified with rationale.
- Ask for and answer questions.

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

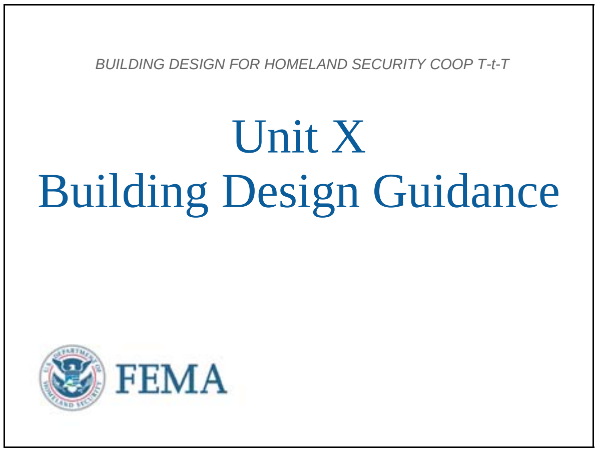
(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

INSTRUCTOR NOTES

VISUAL X-C-1



CONTENT/ACTIVITY

Introduction and Unit Overview

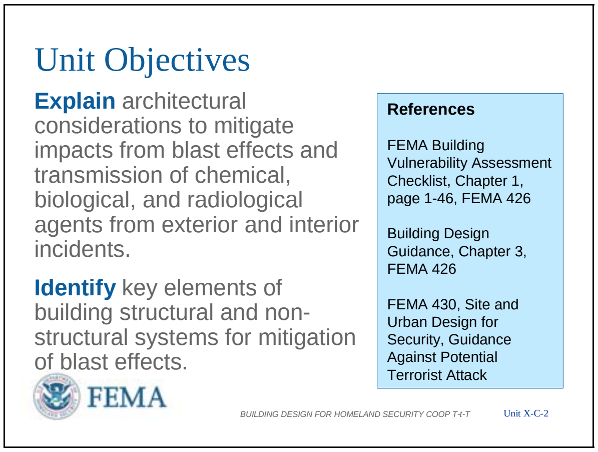
This is Unit X Building Design Guidance. Continuing with our understanding of vulnerability and mitigation measures, we have looked at site and layout concerns and now turn our attention to what considerations are needed in building design to mitigate tactics involving explosive blast or CBR agents.

We will examine design considerations that achieve a balanced building envelope that provides a defensive layer against the given terrorist tactic and avoids creating ripple effects where one incident may affect more than one building system.

Catastrophic collapse of any building is a primary concern. Historically, the majority of fatalities that occur in terrorist attacks directed against buildings are due to building collapse. This was true for the Oklahoma City bombing in 1995 when 87 percent of the building occupants who were killed were in the collapsed portion of the Murrah Federal Building. But glass causes over 80 percent of injuries during bomb blast and there are some low cost techniques to keep CBR agents outside of buildings or to limit their spread inside.

INSTRUCTOR NOTES

VISUAL X-C-2



VISUAL X-C-3

CONTENT/ACTIVITY

Unit Objectives

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

Explain architectural considerations due to impact from blast effects and transmission of chemical, biological, and radiological agents from exterior and interior incidents.

Identify key elements of a building's structural and non-structural systems for mitigation of blast effects.

In addition to FEMA 426, also consult FEMA 430 (future) for additional design concepts.

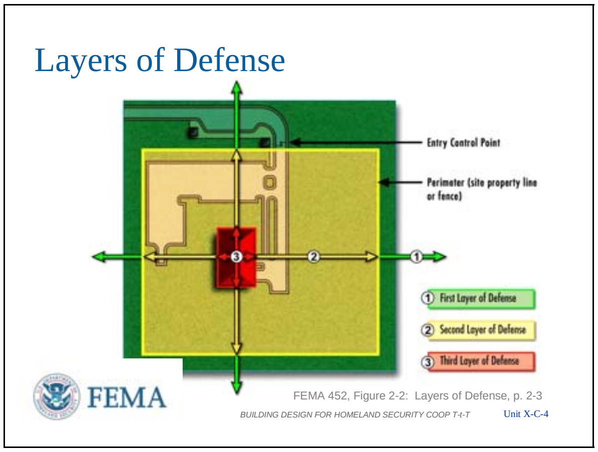
Unit Objectives (continued)

Compare and contrast the benefit of building envelope, mechanical system, electrical system, fire protection system, and communication system mitigation measures, including synergies and conflicts.

Apply these concepts to an existing building or building conceptual design and identify mitigation measures needed to reduce vulnerabilities.

INSTRUCTOR NOTES

VISUAL X-C-4



<u>From FEMA 452</u>
The layers of defense is a traditional approach in security engineering and use concentric circles extending out from an area or site to the building or asset that requires protection. They can be seen as demarcation points for different security strategies. Identifying the layers of defense early in the assessment process will help you to understand better the assets that require protection and determine your mitigation options. Figure 2-2 shows the layers of defense described above.

CONTENT/ACTIVITY

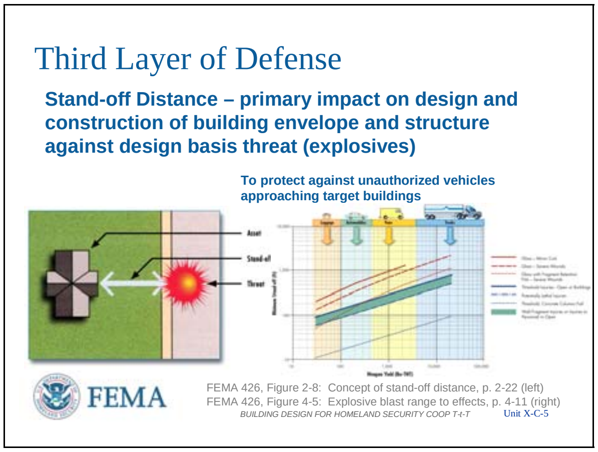
Layers of Defense

The first and second layers were discussed in the previous instruction unit. The Third Layer of Defense is applicable to Building Design – starting at the building drip line, taking into account the complete building envelope, and including any additional considerations found anywhere in the building.

FEMA 452 -- Third Layer of Defense. This deals with the protection of the asset itself. It proposes to harden the structures and systems, incorporate effective HVAC systems and surveillance equipment, and wisely design and locate utilities and mechanical systems. Note that, of all blast mitigation measures, distance is the most effective measure because other measures vary in effectiveness and can be more costly. However, often it is not possible to provide adequate stand-off distance. For example, sidewalks in many urban areas may be less than 10 meters (33 feet), while appropriate stand-off may require a minimum of 25 meters (82 feet). <u>**The building owner has control of this layer and its main mitigation measures are hardening against blast and security sensors/CCTV as final access control.**</u>

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-5



Third Layer of Defense

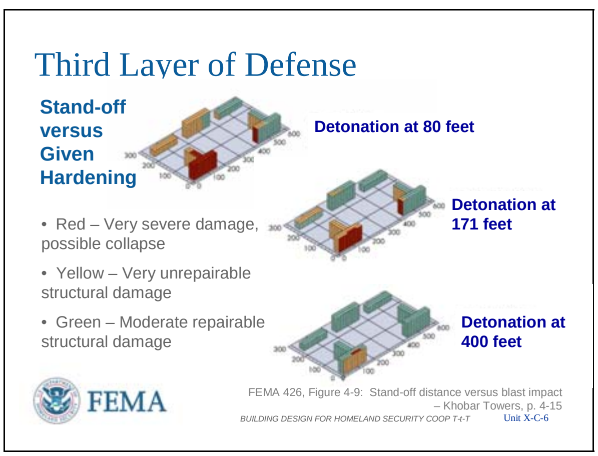
Stand-off Distance versus Hardening of Structures

Of all blast mitigation measures, distance is the most effective measure because other measures vary in effectiveness and can be more costly. However, many times it is not possible to provide adequate stand-off distance.

Desired minimum stand-off in the DoD Unified Facility Criteria (UFC) and used as the initial screening distance in FEMA 426 is 82 feet. However, this may only protect against column collapse for a 250 pound car bomb at 82 feet.

The design basis threat weapon yield and the level of protection desired drive the hardening required for the stand-off distance available.

VISUAL X-C-6



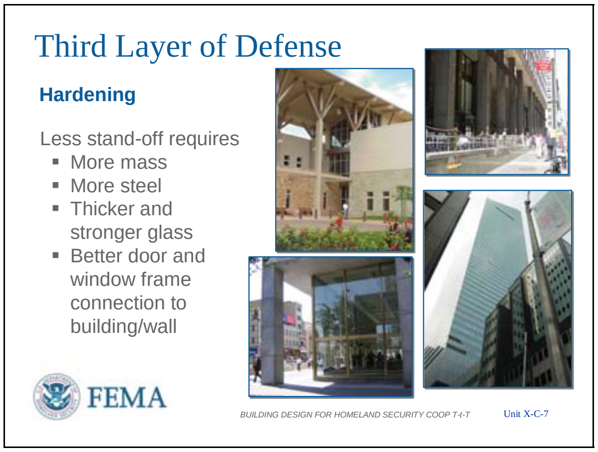
Third Layer of Defense

Stand-off versus Given Hardening

This representation of the estimated damage at Khobar Towers uses the blast modeling software available circa 1997. It shows the front façade of the target building receiving very severe damage when the estimated bomb is at 80 feet. Increasing the stand-off using the same building construction and bomb size shows that the stand-off required to limit damage is 400 feet.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-7



U.S. Embassy: Kampala, Uganda designed to resist explosive blast [upper left – DOS and Hinman]. Other three photos are from New York City indicating glass and overhang (poor) [lower left], similar glass and overhang (poor) but with wall (better) [upper right], and window curtain wall (usually poor) [lower right].

VISUAL X-C-8

Third Layer of Defense

Layers of Defense	Architecture	Structural Systems	Building Envelope	Utility Systems	Mechanical & Electrical Sys	Plumbing & Gas Systems	Fire Alarm Systems	Comm - Info Technology Sys	Equipment Ops & Maint	Security Systems
First Layer										
Second Layer										
Third Layer										

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit X-C-8

Note that one mitigation measure may reduce the risk of more than one asset-threat/hazard pair of interest as illustrated by **Table 2-1, page 2-54, of FEMA 426**, where a mitigation measure may apply to multiple tactics. On

Third Layer of Defense
Hardening

Less stand-off requires more mass and more steel for hardening, thicker and stronger glass, and better window frame connection to the building/wall. However, this should be done in concert with good architecture design and aesthetics principles. As you can see, the other photos show architectural treatments that increase blast damage – overhangs and much glass.

Note that 82 feet of stand-off allows use of conventional construction with minimal upgrades when used in conjunction with a controlled perimeter that detects larger bombs prior to getting anywhere near the building.

Third Layer of Defense

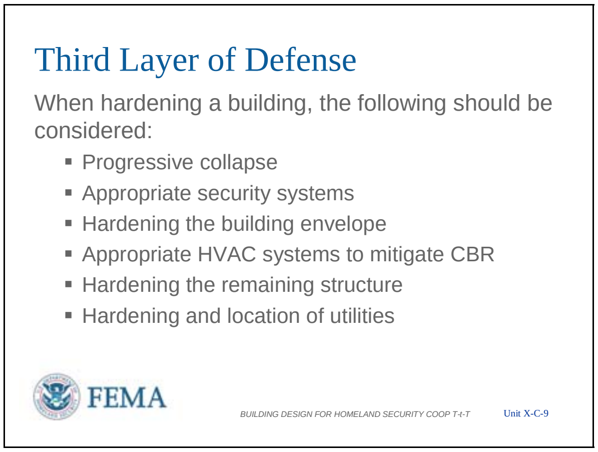
The third layer of defense deals with the protection of the asset itself. The column headings include key elements of protection and the row headings includes the three layers of defense. The matrix allows designers to consider different methods of protection and when they could be used. For the third layer of defense, designers should go through each system to take appropriate mitigation measures for an existing building or provide increased hardening when designing a building.

The rest of this instruction unit will follow along the column headings in the order shown. This is the same order as found in the Building Vulnerability Checklist at the end of Chapter 1 of FEMA 426.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

the other hand, a mitigation measure against one tactic may increase the vulnerability to other tactics.

VISUAL X-C-9



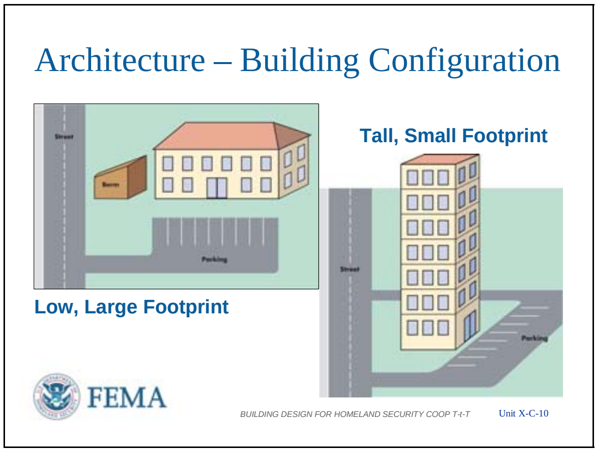
Third Layer of Defense

Hardening Considerations:

- Progressive collapse
  This should be the first consideration as most deaths result from building collapse and life safety seeks to ensure safe evacuation of a building during or after any incident. Structural framing and load-bearing components are the concern here.
- Appropriate security systems
  For an existing building the addition of security systems to deter, detect, and deny the building needs to be done whether or not building hardening can be done.
- Hardening the building envelope
  After progressive collapse, hardening the building envelope provides the most protection against injury during blast events and aligns with building tightness considerations for exterior CBR releases.
- Appropriate HVAC systems to mitigate against CBR
  Next the control of HVAC operation for exterior and interior CBR releases should be considered based upon the complexity of the existing or designed system.
- Hardening the structure
  After progressive collapse and hardening the building envelope, hardening the rest of the structural/nonstructural components to reduce injury should be considered.
- Hardening and location of utilities
  This might be the most expensive to do with an existing building, but should be fully implemented in a new building design. Accessible, aboveground utilities should receive first consideration for hardening.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL X-C-10



Architecture – Building Configuration

Designers should balance a number of relevant considerations to the extent that site, economic, and other factors allow.

Some of the relevant considerations include the following:

- The shape of the building
  - Low, large footprint buildings
  - Tall, small footprint buildings

General benefits of the two basic approaches:

Low, Large Footprint:

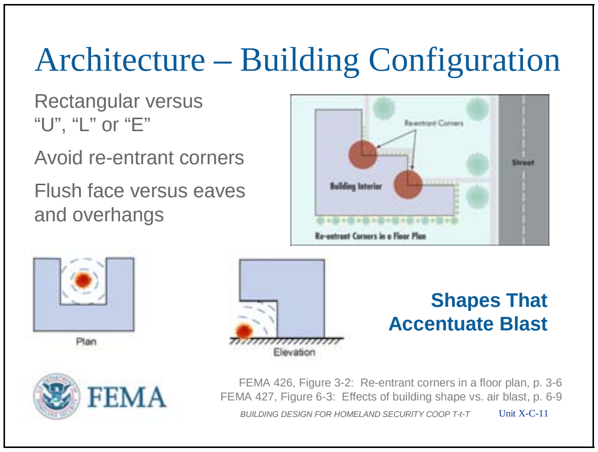
- Reduced effect of explosive blast (catches less of the blast wave) – Dispersed and blast wave rolls over the top.
- Reduced effect of progressive collapse (less of the building can fall) – Due to less structural members impacted.
- Reduced surveillance or easier mitigation (lower height allows terrain and landscaping options)
- Better energy conservation (green roof potential and earth-sheltered design – earth berm reduces energy loss and directs blast wave over the building if the berm is as high as the building)

Tall, Small Footprint:

- Reduced blast effects on upper floors
- Air intakes better protected against CBR events
- Site runoff reduced, reducing culvert size as a covert entry point
- More parking space that meets local planning commission/building code

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-11

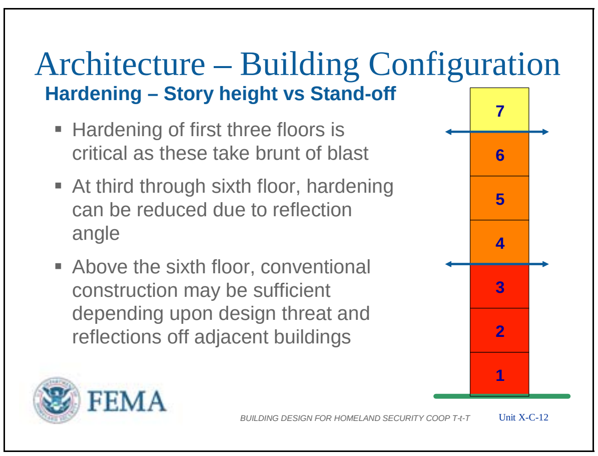


Architecture – Building Configuration

A lot can be done architecturally to mitigate the effects of a terrorist bombing on a facility. These measures often cost nothing or very little if implemented early in the design process. FEMA 430 (future) will contain an expanded discussion of incorporating security components in architectural design.

- Further looking at building shapes, certain configurations trap the blast wave, increasing overall damage to the structure. For example, “U” or “L” shaped buildings, overhangs, and re-entrant corners in general should be avoided. Either the reflected pressure increases as it cannot vent around the building or the building gets hit with reflected blast waves at points already hit by the initial blast wave.

VISUAL X-C-12



Architecture – Building Configuration

GSA has stated the hardening for the urban situation will be fully evaluated for the first three floors of the building because these floors are most vulnerable. At the third through sixth floor, the hardening can be reduced, but some hardening is still necessary. Above the sixth floor may need only conventional construction with minimal hardening -- because the reflection angle is going to result in a lower coefficient of reflection and the increased stand-off distance to these floors also results in less reflected pressure.

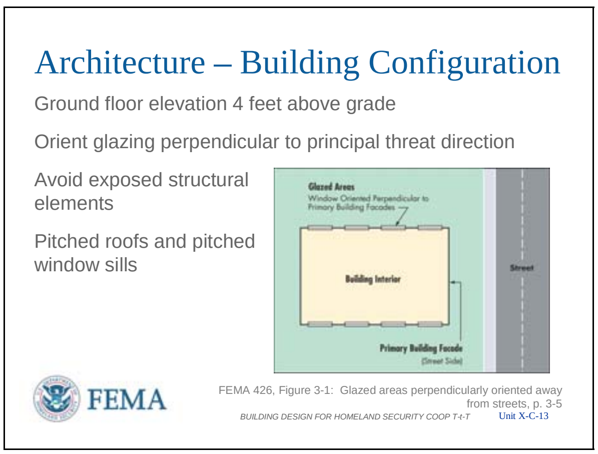
However, as the bomb gets bigger, the upper floors will see severe damage even with the increased reflection angles just due to the higher incident pressure generated by larger bombs.

The GSA approach would hold very well for a

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

high-rise building surrounded by low-rise buildings (3 floors and less), but is probably less applicable for the high-rise building surrounded by other high-rise buildings. Blast wave reflections off adjacent buildings, will affect all floors of the building of interest to varying degrees. The reflections will follow much longer paths resulting in larger effective stand-off distances and the various reflection angles will result in lower incident and reflected pressures compared to the initial blast wave. Unfortunately, the reflections my hit a very weak point in the response motion of the building or building component at any floor level resulting in more damage than would have been originally expected.

VISUAL X-C-13

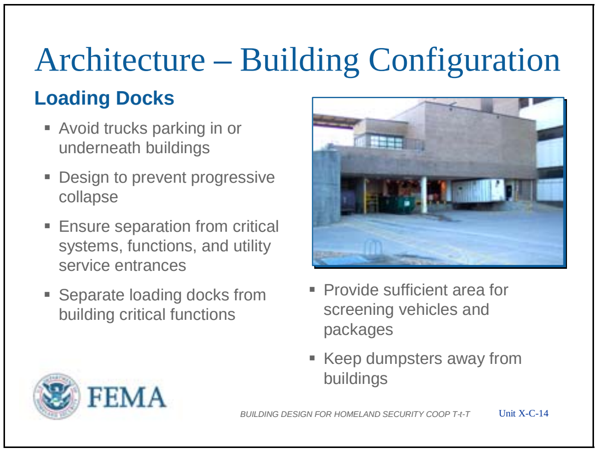


Architecture – Building Configuration

- Elevating the ground floor makes moving vehicle attack more difficult
- If the glazing looks perpendicular to the direction of travel for the blast wave, the glass sees less reflected pressure.
- Do not have structural elements, like columns, easily exposed on the outside of the building. This goes for any architectural feature that can become damaged or disconnected by a blast wave.
- If armed attack includes Molotov cocktails or home-made grenades, pitched roofs and pitched window sills tend to cause the thrown item to roll off and away from the building. Air intakes have similar considerations.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-14
Hidden Slide



Architecture – Building Configuration

Loading Docks

- Loading docks are higher risk locations as larger vehicles with potentially larger bombs are allowed minimal stand-off from the building.
- Building design calls for the basics of preventing progressive collapse, and separating critical equipment, systems, components and functions away from the loading dock.
- Do not provide a hiding location by placing dumpsters adjacent to the building
- Screen packages and vehicles coming to the loading dock at other locations or in an area of sufficient size to allow searches and sufficient distance from the building to reduce the impact of any incident.

VISUAL X-C-15
Hidden Slide

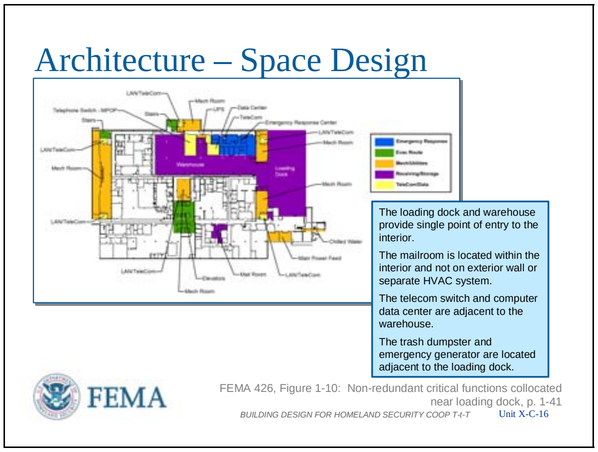
Architecture – Building Configuration

Parking Considerations

- As with loading docks, parking underneath a building is a higher risk situation as larger bombs than can be hand-carried approach the building with minimal stand-off.
- As with loading docks, progressive collapse is a primary concern
- Restrict parking to vetted vehicles, but also provide access control and security systems
- Access from underground parking (stairwells and elevators) to the building should be only to unsecured spaces where access control then occurs, such as outside the footprint of the building

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-16



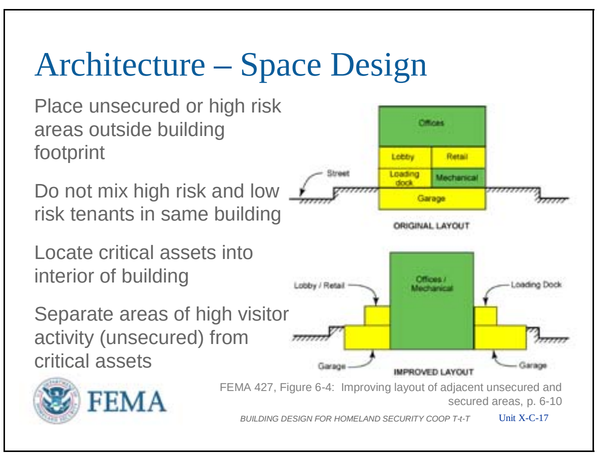
Architecture – Space Design

Functional Layout

Public areas such as the lobby, loading dock, mail room, garage, and retail areas need to be separated from the more secured areas of the facility. This can be done by creating internal "hard lines" or buffer zones, using secondary stairwells, elevator shafts, corridors, and storage areas between public and secured areas.

In lobby areas, the architect would be wise to consider the queuing requirements in front of the inspection stations so that visitors are not forced to stand outside during bad weather conditions or in a congested line inside a small lobby while waiting to enter the secured areas. Consider allowing enough lobby space for future inspection equipment.

VISUAL X-C-17



Architecture – Space Design

Structural Layout

Unsecured areas should be physically separated from the main building to the extent possible.

For example, a separate lobby pavilion or loading dock outside the main footprint provides enhanced protection against damage and potential building collapse in the event of an explosion. Similarly, placing parking areas outside the main footprint of the building can be highly effective in reducing the vulnerability to catastrophic collapse.

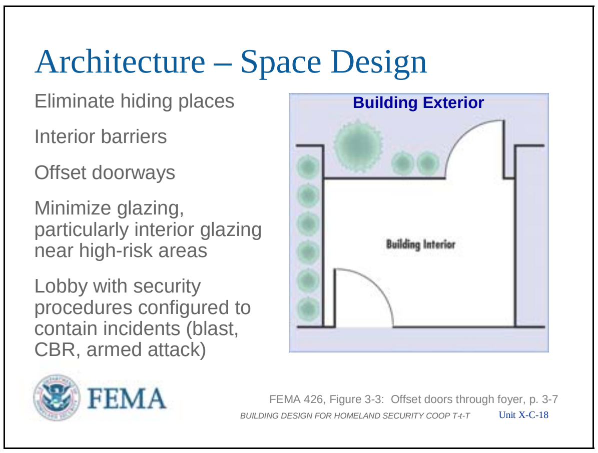
Mixed occupancies. High-risk tenants should not be housed with low-risk tenants. Terrorists may identify some targets based on their symbology, visibility, ideology, political views, potential for publicity, or simply the

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

consequences of their loss. Low-risk tenants are then placed at higher risk due to proximity.

- However, if there are very few high-risk tenants among many low-risk tenants, then dispersal and devalue can be mitigation techniques.
- After Oklahoma City, day care centers (low-risk) are separated from the main building functions (high-risk) to reduce the risk to the day care centers. This has been done at the Pentagon, with a relatively minor decrease in convenience.

VISUAL X-C-18
Hidden Slide



Architecture – Space Design

Design Measures

- Eliminate hiding places
  Generally a good security idea, especially in any areas where few people may frequent, like stairwells or underground parking
- Interior barriers
  Channel building staff and visitors to their respective areas and use interior barriers to provide separation between unsecure and secure areas
- Offset doorways
  If an explosive blast breaches the first door in a foyer, the offset will provide additional protection to the next door -- less incident pressure striking the interior door due to swirling of the blast wave.
- Minimize glazing
  Glass, unless hardened, adds to injuries during incidents. Reducing glazing is one approach, hardening is another, and proper placement is a third.
- Lobby design
  While it is a given that security and access control should be in the lobby, but design should accommodate the occurrence of an incident within lobby – reversal of standard design pressures, containment of the event

INSTRUCTOR NOTES	CONTENT/ACTIVITY

inside the lobby without affecting the rest of the building, control of agents and toxic gases, and hardening against armed attack.

VISUAL X-C-19
Hidden Slide

For additional information on safe havens, see **FEMA 453** - *Design Guidance for Shelters and Safe Rooms: Protecting People Against Terrorist Attacks*

Architecture – Other Location Concerns

When designing high-risk buildings, engineers and architects should consider the following:

The innermost layer of protection within a physical security system is the **safe haven**. Safe havens are not intended to withstand a disciplined, paramilitary attack featuring explosives and heavy weapons. They are locations where sheltering-in-place for CBR, protection from natural hazards or bomb blast can occur.

Offices considered to be high risk (more likely to be targeted by terrorists) should be placed or glazed so that the occupants cannot be seen from an uncontrolled public area such as a street. Whenever possible, these spaces should face courtyards, internal sites, or controlled areas.

Public toilets and service areas, or access to vertical circulation systems (stairwells and elevators) should not be located in any non-secure areas, including the queuing area before visitor screening at the public entrance.

Retail and other mixed uses, which have been encouraged in public buildings by the Public Buildings Cooperative Use Act of 1976, create spaces that are open and inviting. Although important to the public nature of the buildings, the presence of retail and other mixed uses may present a risk to buildings and their occupants and should be carefully considered on a project-specific basis during project design. Consider allowing access to retail space only from the outside of the building and not between any interior spaces

INSTRUCTOR NOTES	CONTENT/ACTIVITY

or consider access configuration so that movement from retail spaces must go past security to get to the rest of the building.

Stairwells required for emergency egress should be located as remotely as possible from areas where blast events might occur and, wherever possible, should not discharge into lobbies, parking, or loading areas. When possible, emergency egress stairwells should be separate from the main building ingress stairwells, and secured to prevent individuals from accessing the secured floors of the building. Also do "What-If" as what would be done if a stairwell is lost as an egress during an incident.

Mailrooms should be located away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets. Avoid locating a mailroom in the same building as a child care center. In fact, the processing and inspection of mail and packages is best done in a separate building if possible. If an incident requires evacuation of the building, a separate building would limit the impact, vice a high-occupancy office building. Ditto, do "What-If" and plan alternatives.

VISUAL X-C-20

Structural Systems

Progressive Collapse Design

Progressive collapse is a situation where local failure of a primary structural component leads to the collapse of adjoining members, which, in turn, leads to additional collapse. Hence, the total damage is disproportionate to the original cause. Progressive collapse is a chain reaction of structural failures that follows from damage to a relatively small portion of a structure. More information on progressive collapse can also be found in

INSTRUCTOR NOTES

To minimize the potential for **progressive collapse**, designers should understand the following:

- The use of **redundant** lateral and vertical load paths is highly encouraged.
- Ductile materials are needed for both primary and secondary structural elements to be capable of deforming well beyond the elastic limit.
- Both the primary and secondary structural elements should be designed to resist load reversals.
- Primary structural elements should be able to resist shear failures by having flexural capacity greater than shear capacity.
- Fire protection should be applied to structural members to survive a worst-case fire duration allows fire fighters to control damage prior to initiation of structural collapse. Suggest reviewing the National Institute of Standards and Technology (NIST) report dealing with World Trade Center 7 (WTC 7) which collapsed due to fire.

CONTENT/ACTIVITY

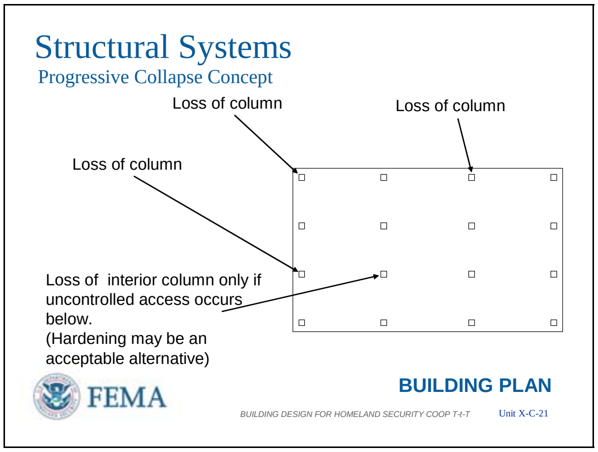
FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks.*

Buildings should be designed with the intent of reducing the potential for progressive collapse as a result of an abnormal loading event, regardless of the required level of protection.

- Primary structural elements are columns girders and roof beams that are the first items for design to prevent progressive collapse.
- Secondary structural elements, such as floor beams and slabs, also may contribute to progressive collapse. Of particular weakness to progressive collapse is flat slab construction where the floor is thickened in areas to substitute for beams in the interest of cost savings. Floor connections to columns are the concern in this type of construction. This has been a standard office building design for many years, but should not be used if progressive collapse is a concern.
- Primary nonstructural elements, such as ceilings and heavy suspended mechanical equipment, contribute to casualties but not progressive collapse.
- Secondary nonstructural elements, such as partitions, furniture, and light fixtures, like primary nonstructural elements, also contribute to casualties, but not progressive collapse.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-21



Structural Systems

Progressive Collapse Concept

The GSA and DoD require that the structural response of a building be analyzed in a methodology that removes a key structural element (e.g., vertical load carrying column, section of bearing wall, beam, etc.) to simulate local damage from any incident. If effective alternative load paths are available for redistributing the loads that was originally supported by the removed structural element, the building has a low potential for progressive collapse.

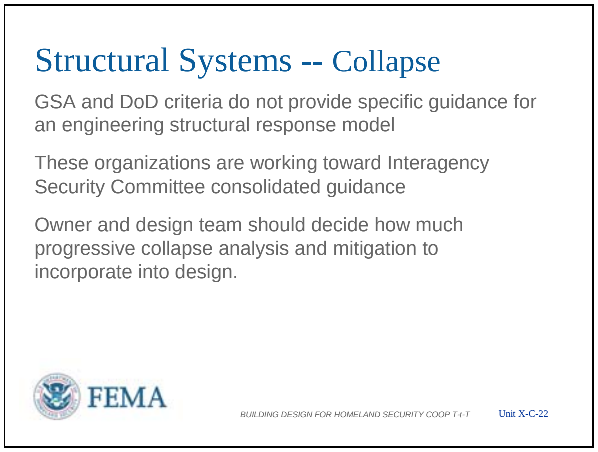
- If a column is lost, will the rest of the building still stand?
- If an exterior beam is lost, will the rest of the building still stand?
- If connections between column and floors are lost will the slenderized column still be able to carry the load or if the column fails, will the rest of the building still stand? DoD criteria states that columns of high-occupancy buildings will remain standing if all the floor connections on a given floor connecting to that column are lost.

If the threat can get to an interior column or beam, the same questions apply, such as underground parking or a mailroom.

Note that the more complex the structure layout (differing from square or rectangle) the more components (columns and beams) that must be analyzed.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-22
Hidden Slide

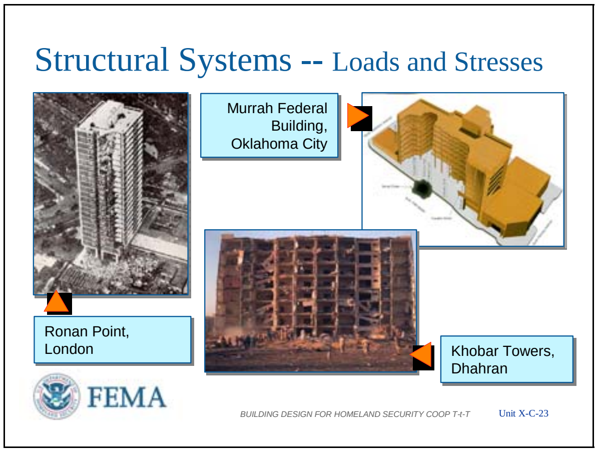


Structural Systems -- Collapse

- Although these criteria provide specific guidance on which structural elements must be analyzed for removal from the structural design configuration, they do not provide specific guidance for choosing an engineering structural response model for verifying the effectiveness of alternate load paths.
- Unless a building is being designed to meet the GSA or DOD criteria, it is up to the owner and the design team to decide how much progressive collapse analysis and mitigation to incorporate into their design.
- Priority should be given to the critical elements that are essential to mitigating the extent of collapse. Designs for secondary structural elements should minimize injury and damage.
- Consideration should be given to reducing damage and injury from primary as well as secondary nonstructural elements.

Both GSA and DoD take a threat-independent approach to progressive collapse – it does not matter how the column or beam is damaged or removed, the intent is that the building will remain standing. However, the concept is a single structural member being removed – if the Design Basis Threat is large enough to damage two components simultaneously, then additional analysis would be needed.

VISUAL X-C-23



Ronan Point: On the morning of 16 May 1968, Mrs. Ivy Hodge, a tenant on the 18th floor of the 22 (24 in other reports) -story Ronan Point apartment tower in Newham, east London, struck a match in her kitchen. The match set off a gas explosion that knocked out load-bearing precast concrete panels near the corner of the building. The loss of support at the 18th floor caused the floors above to collapse all the way to the roof.

The impact of these collapsing floors set off a chain reaction of collapses almost all the way to the ground. The ultimate result can be seen in Figure 1: the corner bay of the building has collapsed from top to bottom. Mrs. Hodge survived but four others died.

Construction of Ronan Point primarily consisted of precast concrete panels. While this type of construction can be designed to avoid progressive collapse from abnormal loading conditions, Ronan Point lacked the connection details necessary to effectively redistribute load. The essential missing detail was reinforcement continuity between panels. Because of this, there was no mechanism in place for achieving effective alternate load

Structural Systems -- Loads and Stresses

The DoD designates the level of blast protection a building must meet based on how many occupants it contains and its function. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads.

Ronan Point had a whole section of the building collapse due to load-bearing precast concrete panels in one apartment being lost. That incident changed the British Code to prevent similar occurrences.

Khobar Towers was designed to the British Code, and only the façade was lost.

The Murrah Federal Building was not designed to the British Code and the loss of one column then affected a transfer girder. There were discontinuities in columns across the lobby causing multiple columns to fail when the transfer girder became unsupported, resulting in load transfers that the building could not handle.

The minimum goal is to have continuous columns from foundation to roof. When assessing a building any discontinuity of columns is a flag indicated the need for further analysis.

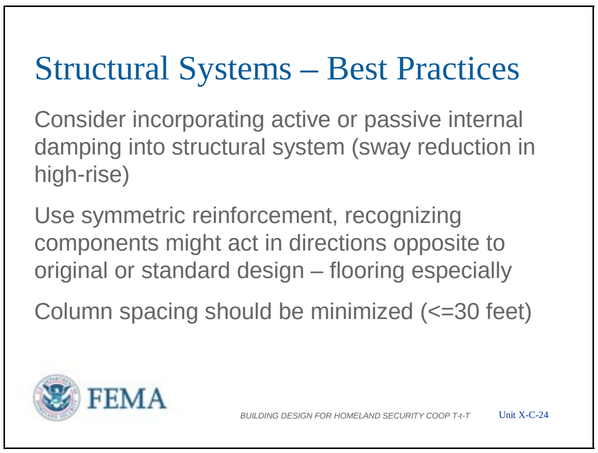
INSTRUCTOR NOTES

paths once failure began to propagate.

Khobar Towers was built to the British Standard that was a result of Ronan Point.

The Murrah Building owner wanted no columns in the lobby, thus designer used transfer beams to carry the load of the upper columns.

VISUAL X-C-24



CONTENT/ACTIVITY

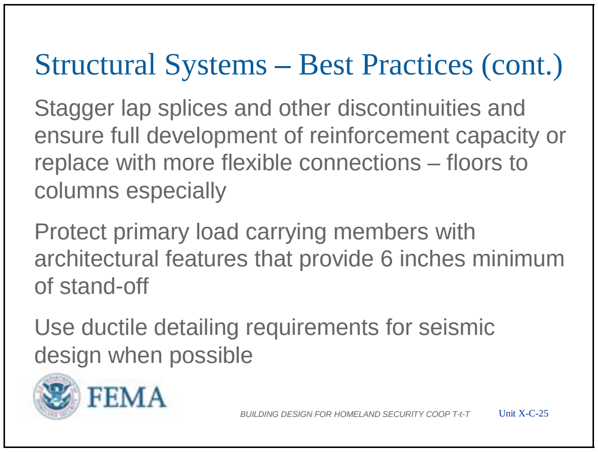
Structural Systems – Best Practices

The following guidelines are commonly used to mitigate the effects of blast on structures and to mitigate the potential for progressive collapse. These guidelines are not meant to be complete, but are provided to assist the designer in the initial evaluation and selection of design approaches. For example:

- Consider incorporating internal damping into the structural system to absorb the blast impact. Although mass has been the blast design approach in the past, using more ductile materials with damping is being investigated. Damping systems will most likely be found in high-rise buildings.
- The use of symmetric reinforcement can increase the ultimate load capacity of the structure. This is especially true for load reversals on floor slabs.
- A practical upper level for column spacing is 30 feet, but 20 feet is better. If the column is lost, the remaining beam must span 40 to 60 feet. Above 60 feet, the beam becomes unreasonably large and expensive. Note that the Murrah Building had 40-foot column spacing in the lobby.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

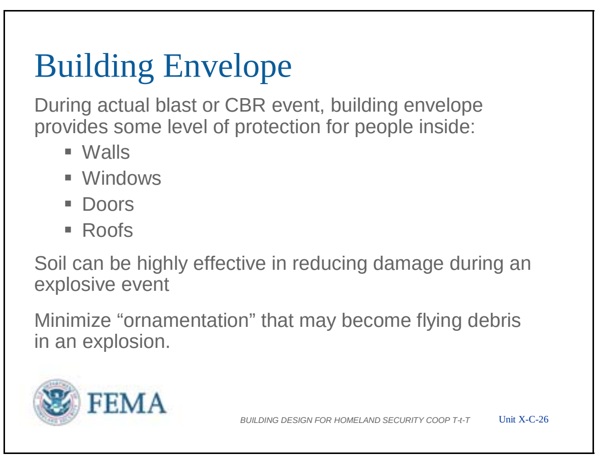
VISUAL X-C-25



Structural Systems – Best Practices (cont.)

- Lap splices must be upgraded from those found in conventional construction to handle the forces during a blast event. Consider interlocking "J" splices.
- By keeping a 6-inch stand-off from vertical load carrying members, a small weapons charge is less likely to shear the member.
- In many cases, the ductile detailing requirements for seismic design and the alternate load paths provided by progressive collapse design assist in the protection from blast.
- Ductility can be imbedded in the material, like steel reinforcing of concrete, or added to an existing component, like fragment-retention film on windows or spray-on truck bed liner on walls to strengthen weaker structures and catch fragmentation.

VISUAL X-C-26



Building Envelope

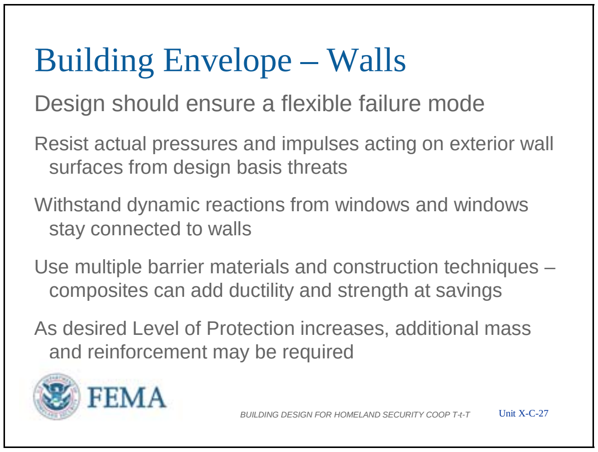
General principles:

- The exterior envelope of the building is the most vulnerable to an exterior explosive threat because it is closest to the blast.
- The exterior envelope also impacts the infiltration of CBR agents into the structure, but tight building construction must be done in conjunction with other actions to ensure some level of protection
- Soil can be highly effective in reducing the impact of a major explosion by reducing fragmentation off walls and street furniture or directing a blast wave over a building.
- Minimize "ornamentation" that may become flying debris in an explosion. This

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

includes street furniture, overhangs, sculptures, etc.

VISUAL X-C-27
Hidden Slide



Building Envelope – Walls

Ideally, the exterior walls need to be able to resist the loads transmitted by the windows and doors. It is not uncommon for bullet-resistant windows to have a higher ultimate capacity than the walls to which they are attached.

Beyond ensuring a flexible failure mode, design the exterior wall to resist the pressure levels of the design basis threat. Special reinforcing and anchors should be provided around blast-resistant window and door frames.

Deflections around certain members, such as windows, should be controlled to prevent premature failure. Additional reinforcement is generally required. Window frame deflection must not cause premature window glazing failure and window frame deflection must not differ greatly from the wall deflections. Seismic pinning of window frames may be required.

Poured-in-place reinforced concrete will provide the highest level of protection, but solutions like pre-cast concrete, reinforced CMU block, metal studs, and a combination of these may also be used to achieve lower levels of protection. Connections are the key, especially for pre-cast concrete curtain walls.

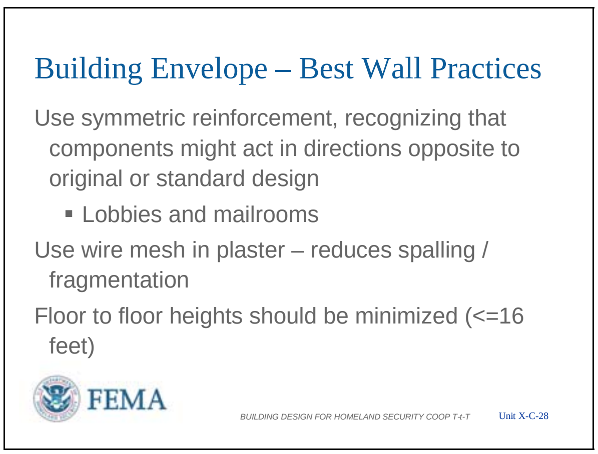
Retrofitting existing unreinforced masonry walls may consider steel plates, metal studs, reinforced concrete backing wall, high-strength fibers glued to the wall, or spray-on truck bed liner. If the wall is double-wythe (two wall system) – usually a brick exterior, air gap, and interior CMU block, consider

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

spraying vermiculite into the air gap to add mass and ductility.

When the design basis threat increases or the level of protection desired increases, the solution is more mass and more reinforcement to add ductility. Increasing the ductility of exterior walls along with mass are suitable ways to ensure blast pressure and fragmentation do not readily enter the building.

VISUAL X-C-28



Building Envelope – Best Wall Practices

The following best practices are commonly used to mitigate the effects of blast on structures and to mitigate the potential for progressive collapse. These guidelines are not meant to be complete, but are provided to assist the designer in the initial evaluation and selection of design approaches. For example:

Just as mentioned with structural framing, symmetrical reinforcement adds strength to masonry and concrete walls, especially on the side away from the bomb where the reinforcement increases the tensile strength of the concrete. Thus, for lobbies and mailrooms the bombs can be exterior (where standard design places wind loading, rain, snow, and flying debris) or interior, so the symmetric reinforcement adds strength to the wall in either direction.

Wire mesh keeps plaster together, adds tensile strength, reduces spalling of the plaster, and assists in keeping fragmentation from entering the room (plaster or otherwise).

In general, floor to floor heights should be minimized. Unless there is an overriding architectural requirement, a practical limit is generally less than or equal to 16 feet. Consider bond beams (which connect

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-29

Building Envelope – Best Wall Practices (cont.)

Connect façade from floor slab to floor slab to avoid attachments to columns (one-way wall elements)

- Limits forces transferred to vertical structural elements

No unreinforced CMU – use fully grouted and reinforced construction

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T

Unit X-C-29

columns at about the mid-point between floor or run across the top of doors and windows), as used in seismic zones, to reduce the effective height of the wall. Since the walls are connected to the floor above and below, the shorter the wall height the stronger the wall all other things being equal.

Building Envelope – Best Wall Practices (cont.)

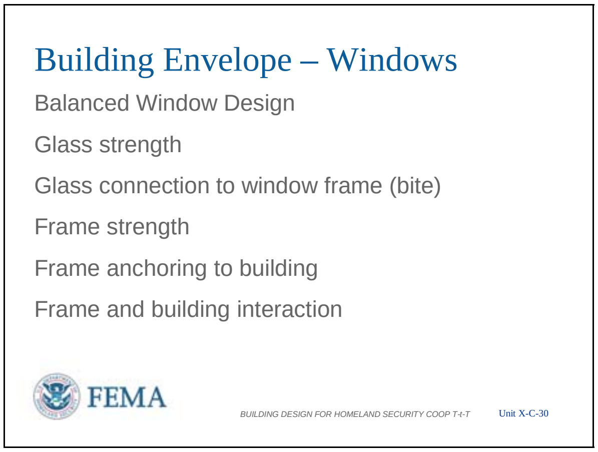
Additional best practices include:

The reason why the walls are connected to the floor above and the floor below is to ensure there is no direct loading on the columns. Since the walls are only pinned at the top and the bottom this is called one-way. If they were also pinned to the columns on each side they would be two-way wall elements. Good blast design seeks to keep the structural framing as the absolute last component of the building to fail, thus the use of one-way wall elements.

Avoid the use of unreinforced masonry when blast is a threat. Masonry walls break up readily and become secondary fragments during blasts. Grout (mass) and reinforcement (ductility) are definitely required for blast resistance. The Ufundi building next to the Kenya embassy was all unreinforced brick and the bomb blast toppled the whole building.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-30



Building Envelope – Windows

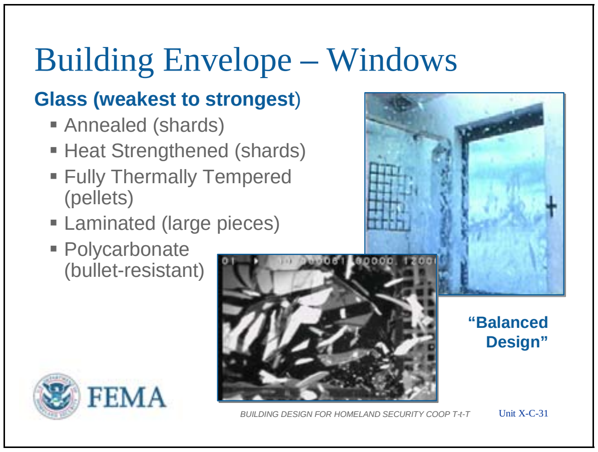
Window systems on the exterior façade of a building should be designed to mitigate the hazardous effects of flying glass during an explosion event. Designs should integrate the features of the glass, connection of the glass to the frame (bite), and anchoring of the frame to the building structure to achieve a "balanced design." This means all the components should have compatible capacities and theoretically would all fail at the same pressure-pulse levels. In this way, the damage sequence and extent of damage are controlled.

Ultimately, in a "balanced" design, the order of failure should be:

- Glass
- Window frame and frame anchoring
- Wall
- Building structural framing

The pressure differences should not be large and the Level of Protection for the Design Basis Threat should be met.

VISUAL X-C-31



Building Envelope – Windows

Five types of glass are commonly used in window glazing systems: annealed glass, heat strengthened glass, fully thermally tempered, laminated glass, and polycarbonate. Other types of glass materials exist, but are not commonly used in typical commercial window systems. Of the five common types, **annealed glass** and **fully thermally tempered glass** are the type of windows for most office buildings.

Annealed glass, also known as float, plate, or sheet glass, is the most common glass type used in commercial construction. Annealed

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

glass is of relatively low strength and, upon failure, fractures into razor sharp, dagger-shaped fragments (see slide -- the right photo is annealed glass failing during an actual explosive test and the left photo is a close-up of the shards). Annealed glass breaks at about 0.2 psi (incident pressure).

Heat strengthened glass (HS), also known as double strength glass, is used where wind loading starts becoming a problem. It breaks like annealed glass, but at about 0.4 psi (incident pressure).

Fully thermally tempered glass (TTG) is typically four to five times stronger than annealed glass. Instead of shards, TTG breaks into pellets that can be stopped by a regular suit coat. It breaks at about 0.8 psi (incident pressure.

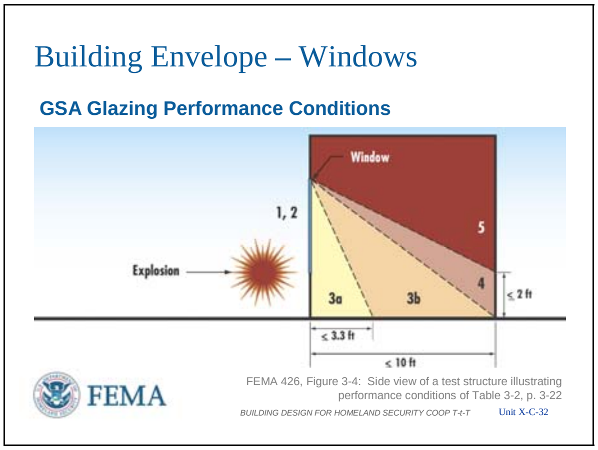
Laminated glass is a pane with multiple glass layers and a pliable interlayer material (usually made from polyvinyl butyral (PVB)) between the glass layers. This interlayer should have a thickness of 30 mils [30 thousandths of an inch] (minimum) or 60 mils (recommended). Do not use an interlayer of 15 mils.

Thermoplastic polycarbonates are very strong and suitable for blast- and forced entry-resistant window design. They are usually laminated in 3 or more layers with glass on the outside to prevent environmental degradation of the plastic (yellowing) and to aid in cleaning (avoid scratches).

Wire-reinforced glass is a common glazing material. It consists of annealed glass with an embedded layer of wire mesh. It is usually used for fire resistance and as a forced entry barrier. It is not recommended for blast design.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-32



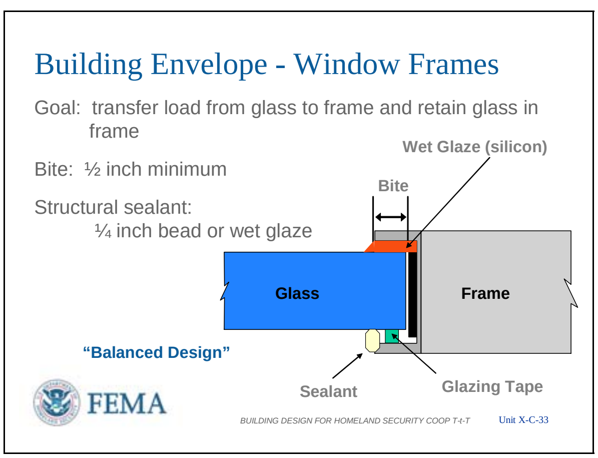
Building Envelope – Windows

GSA Glazing Performance Conditions

Table 3-1, page 3-21, in FEMA 426 presents six GSA glazing protection levels based on how far glass fragments would enter a space and potentially injure its occupants (known as a flight model). This slide depicts how far glass fragments could enter a structure for each GSA performance condition. The divide between performance conditions 3a and 3b can be equated to the “threshold of injury.” The divide between performance conditions 4 and 5 can be equated to the “threshold of lethality.” A person standing in the room has a potential of being hit in the upper body/head area by glass fragments that are traveling fast enough to penetrate the body.

The GSA glazing performance conditions shown will correlate with the DoD levels of protection presented in **Table 3-2, page 3-22, in FEMA 426** as shown previously in Unit VII, Explosive Blast.

VISUAL X-C-33



Building Envelope -- Window Frames

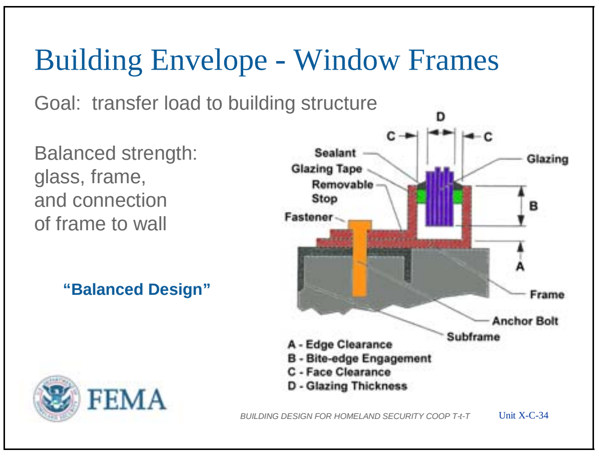
Window frames need to retain the glass so that the entire pane does not pull out (glass flexes and can pull out of frame during the blast) and also should be designed to resist the breaking stress of the window glass.

The window bite (i.e., the depth of window captured by the frame) needs to be at least ½ inch. DoD criteria call for a minimum 3/8-inch bite if silicon sealant is applied, but call for a 1-inch bite if no silicone sealant is used. Butt-glazed strip windows can require even more bite with or without sealant, since there is bite only on the top and bottom of the window.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

To retain the glass in the frame, a minimum of a ¼-inch bead of structural sealant (i.e., silicone or polyvinyl butyral) should be used around the inner perimeter of the window. This should be done on all four sides of the window. Since strip windows with butt glazing can only apply sealant on the top and bottom, they are not good options for blast as the bite must be large, even with sealant.

VISUAL X-C-34



Window Frames

The frame must not flex during the blast loading and cause the glass to pop out.

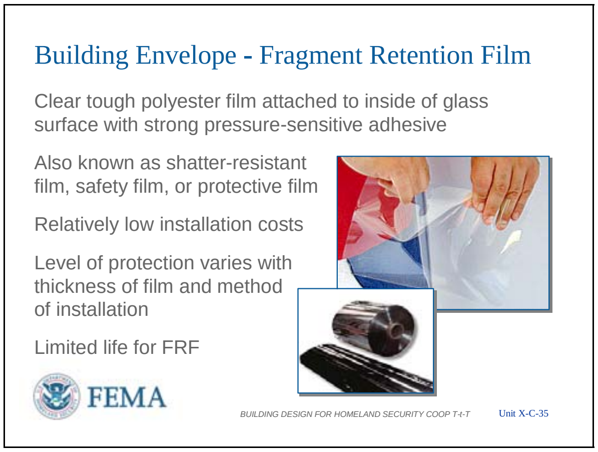
The blast loading across the glass and frame now transfers to the frame connections to the building. These connections must handle the <u>shear</u> and <u>tensile</u> stresses and the <u>bending moments</u> of the connection design.

The frame members connecting adjoining windows are referred to as mullions. These members may be designed using a static approach when the breaking strength of the window glass is applied to the mullion, or a dynamic load may be applied using the peak pressure and impulse values. Because mullions only connect at their top and bottom ends to the building structure, the mullion must handle the transferred blast loading from both adjacent windows.

Other considerations for windows must balance the amount of light, energy conservation, noise transmission, venting of fumes, and emergency egress in addition to blast response and CBR protection.

INSTRUCTOR NOTES

VISUAL X-C-35
Hidden Slide



When obscuration of rooms cannot be handled by site and layout design, one alternative is to install glazing with mirrored finishes or add fragment retention film that is mirrored. This works fairly well with single pane windows, but double pane windows may overheat with the mirrored fragment retention film – consult window manufacturer if there is a question. Realize, however that the mirrored finishes work best during daytime ambient light (room light less bright compared to ambient light). At night time or on overcast days, observation into the room is possible if interior lights are on. Shades or Venetian blinds can provide obscuration during low ambient light.

CONTENT/ACTIVITY

Building Envelope – Fragment Retention Film (FRF)

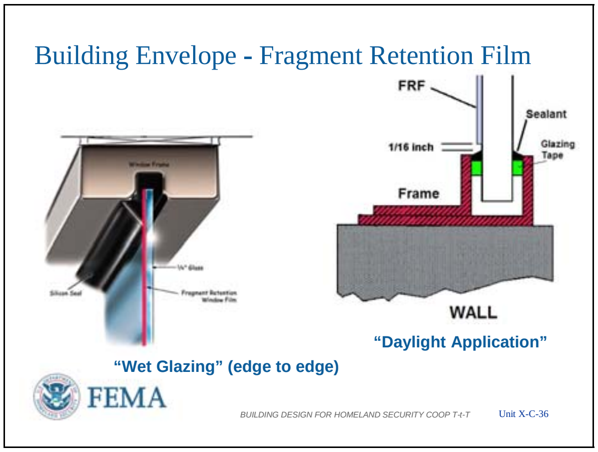
Another treatment used for mitigating the effects of an explosive attack is **security window film.** The polyester film used in commercial products is commonly referred to as fragment retention film (FRF), safety film, security film, protective film, or shatter-resistant film. These films adhere to the interior surface of the window to provide fragment retention and reduce the overall velocity of the glass fragments at failure. The film greatly increases the tensile strength of thin annealed glass and limits the deflection of the glass under blast loading.

Fragment retention film combines a strong pressure sensitive adhesive with a tough polyester layer. It should be limited to use in retrofit applications due to degradation of the film and adhesive by ultraviolet light. Do not use for new construction and it is of little to negative benefit on thicker, higher strength glass. For example, applying FRF to 3/8-inch thermally tempered glass will INCREASE the stand-off required for a given bomb size as the film will hold the glass together, acting like a sail and increasing the distance that the glass will fly into the test room.

Note that fragment retention film can be justified for multiple reasons – blast protection, physical security (smash and grab), and energy conservation (mirrored or tinted). Thus, justification can be based upon the multiple benefits derived for little difference in cost.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-36



Building Envelope – Fragment Retention Film

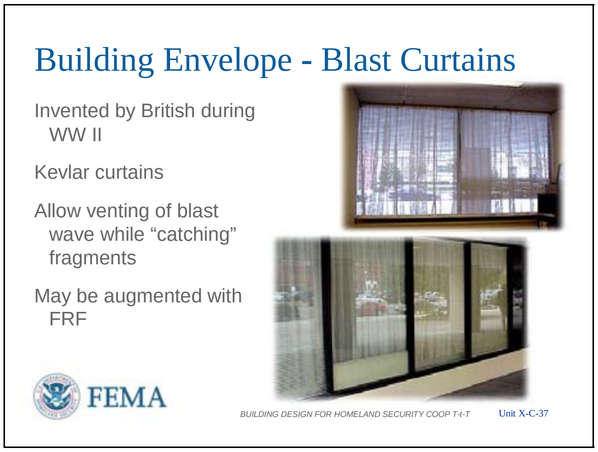
Fragment retention film behaves similarly to relatively thin laminated and polycarbonate glazing in terms of fragmentation. It is available in common thicknesses of 2, 4, 7, and 10 mils. Also found up to 15 mils. The Navy recommends 10 mils.

Fragment retention film improves the performance of the glass under blast loading to varying degrees, depending on the thickness, quality, and type of film installation. Note a daylight application will leave a 1/16 inch space around the edge of the FRF where water used to apply the FRF is squeegeed out. Daylight application of FRF to very thin glass can reduce the stand-off distance in half for a given level of protection. The best performance is achieved when the film is installed into the bite of the glazing or is connected to the frame (mechanically or with chemical sealants).

Fragment retention film can also be purchased with tinted, mirrored, or solar versions that provide energy conservation benefits when using air conditioning.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

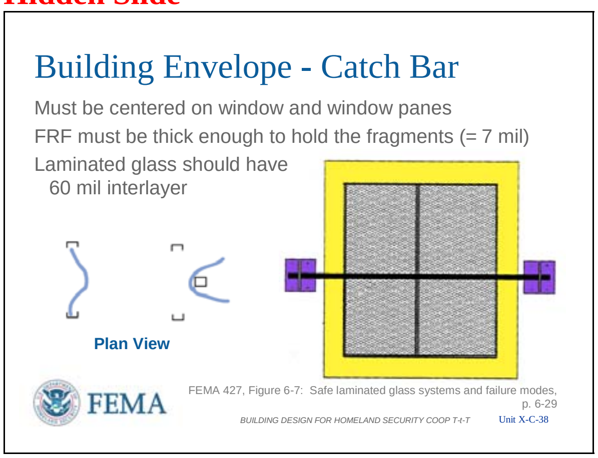
VISUAL X-C-37
Hidden Slide



Building Envelope – Blast Curtains

- Can now see out of these curtains as opposed to the "blackout" curtains from WWII -- uses Kevlar or other high strength fibers. In fact it is easier to see out of sheer black curtains than sheer white curtains.
- They allow venting of the blast wave while "catching" glass fragments
- May be augmented with FRF (British only specify them with FRF)
- Connections of curtains or blast shields to building frame are critical.

VISUAL X-C-38
Hidden Slide



Building Envelope – Catch Bar

Increased safety for fragment retention can be obtained in the event of catastrophic failure from an explosive blast by placing a decorative catch bar or grillwork on the interior of the glazing. Note, catch bars must be mounted across the center of mass of each window pane (vision area of glass) to be effective. A catch bar is ineffective with 4 mil FRF as the FRF will just tear (shear) on the catch bar. This is also another reason why the Navy recommends 10 mil.

Catch bars are usually considered with a retrofit of fragment retention film to not only catch the glass, but also catch the existing window frame that may not be adequately connected to the wall. They can also be considered for laminated glass.

INSTRUCTOR NOTES

VISUAL X-C-39

Building Envelope – Best Window Practices

No windows adjacent to doors

Minimize number and size of windows - watch building code requirements

Laminated glass for high-occupancy buildings

Stationary, non-operating windows, but operable window may be needed by building code

Steel versus aluminum window framing

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit X-C-39

CONTENT/ACTIVITY

Building Envelope – Best Window Practice

Windows adjacent to doors allow easy access to the locking mechanism on the door by just breaking the window and reaching in.

Smaller windows are stronger against blast for a given window material and less expensive as well. Using fewer windows also reduces cost. However, building codes may specify the square footage of windows required based upon the total square footage of the floor level the windows are on.

Laminated glass is required for high-occupancy buildings by DoD. For life cycle costing and blast resistance, especially at the lower end of weapon yield, laminated glass is the best choice.

Life safety/fire codes may require operable windows as an escape route in certain occupancies (dormitories, for example). Recommend sliding or swing-out windows for better blast performance.

Heavy duty aluminum frames have performed well, although steel should be specified if design basis threat is large.

INSTRUCTOR NOTES

VISUAL X-C-40

Building Envelope – Doors

Balanced strength
- Door
- Frame
- Anchorage to building

Hollow steel doors or steel-clad doors

Steel door frames

Blast-resistant doors available
- Generally heavy
- Generally expensive

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit X-C-40

CONTENT/ACTIVITY

Building Envelope – Doors

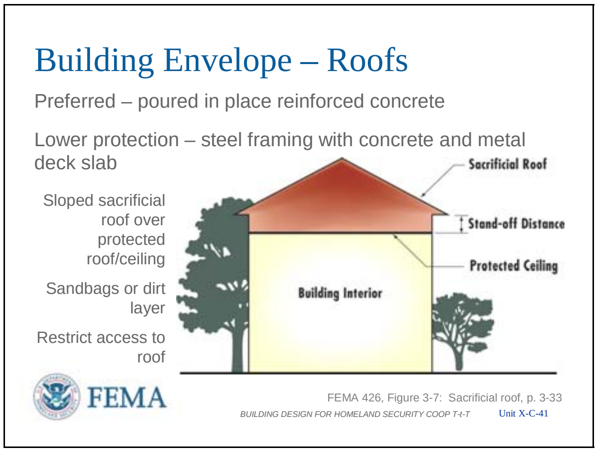
A door system includes the door, frame, and anchorage to the building. As part of a balanced design approach, exterior doors in high risk buildings should be designed to withstand the maximum dynamic pressure and duration of the load from the design threat explosive blast. Other general door considerations are as follows:

Provide hollow steel doors or steel-clad doors with steel frames.
Provide blast-resistant doors for high threats and high levels of protection.
Limit normal entry/egress through one door, if possible.
Keep exterior doors to a minimum while accommodating emergency egress.
Ensure that exterior doors open outward from inhabited areas. If inward opening the locking mechanism must handle the blast loading [A 3 foot by 7 foot door has 3 x 7 x 144 = 3,024 square inches of surface area. A reflected blast pressure of 2 psi puts <u>3 tons of force</u> on that locking mechanism.] If outward opening the whole door frame takes the blast loading.
Replace externally mounted locks and hasps with internally locking devices because the weakest part of a door system is the latching component.
Install doors, where practical, so that they present a blank, flush surface to the outside to reduce their vulnerability to attack.
Locate hinges on the interior or provide concealed hinges to reduce their vulnerability to tampering. [Ask students if they see anything wrong with the door in the photo – exterior hinges. However, there is a balanced magnetic switch on the inside of the door connected to the security alarm which mitigates the exterior hinges.
Install emergency exit doors so that they facilitate only exiting movement.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Equip any outward-opening double door with protective hinges and key-operated mortise-type locks.
Provide solid doors or walls as a backup for glass doors in foyers.

VISUAL X-C-41



Building Envelope – Roofs

For an explosive threat, especially for thrown explosives (e.g., satchels, hand grenades, and even mortars), the primary loading on the roof is downward over-pressure. The stand-off to the protected ceiling provides the protection. The sloped roof tends to cause the explosive to roll off and away from the building. For explosions at ground level, secondary loads include upward pressure on the protected ceiling and roof due to the blast penetrating through openings and upward suction during the negative loading phase. The upward pressures may have an increased duration due to multiple reflections of the air blast internally. It is conservative to consider the downward and upward loads separately.

The preferred system is to use poured-in-place reinforced concrete with beams in two directions. If this system is used, beams should have stirrups along the entire span spaced not greater than one half the beam depths. Steel pan formwork provides additional protection as the formwork mitigates falling debris, but since load reversals may occur, the concrete in the steel pan formwork should have steel in both faces (symmetrical reinforcement).

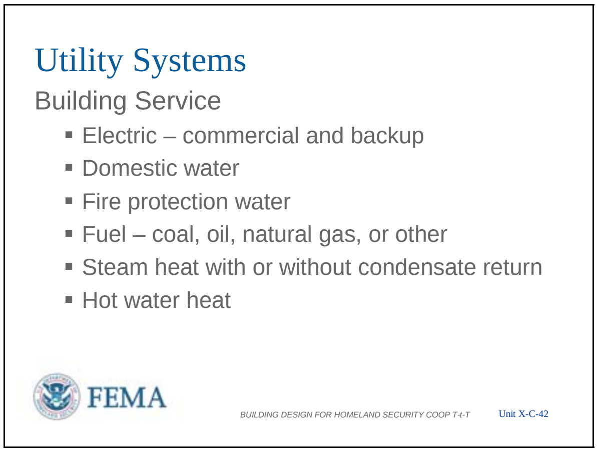
Less desirable systems include metal plate systems without concrete, and precast and pre/post tensioned systems.

<u>Precast roof panels</u> are problematic because of the tendency to fail at the connections, like pre-cast curtain walls.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**
	<u>Pre/post tensioned systems</u> tend to fail in a brittle manner if stressed beyond their elastic limit and they also are not able to accept upward loads without additional reinforcement. Standard construction found in the Middle East, for example, uses soil/dirt as insulation in the roof at a thickness of 18 inches or so. The soil is placed on a waterproofed concrete poured-in-place deck and covered with 1-meter square concrete panels that are waterproofed and sloped to roof drains. With two layers of standard sand bags (about 8 inches in total deep) on top, this roof, has a high level of protection. Many conventional roof designs will provide a suitable blast response for most buildings, considering minimum Design Basis Threats. The intent here is to point out what roofs may be a problem and why. For higher Design Basis Threats and tactics involving the roof, the protected ceiling and sacrificial roof concept applies.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-42



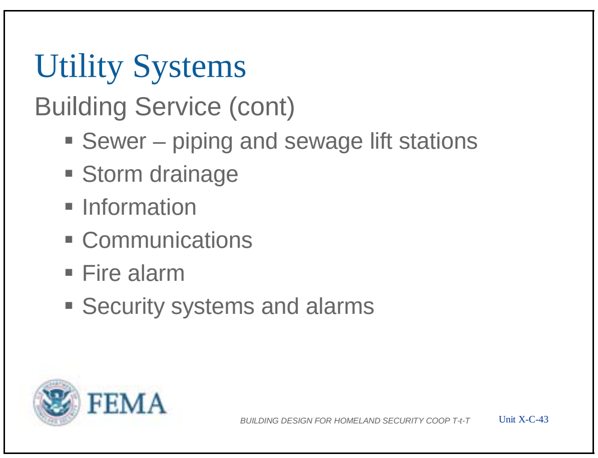
Utility Systems

Building Service

While Utility Systems are first and foremost considered under Site and Layout Design, they have a direct impact on the building envelope based upon where and how they enter the building to provide service to that structure. While most will think of what is brought into a building, it is equally important to note what needs to be taken out of the building to maintain function and operation.

For example, steam heat may be provided by a central boiler plant on the site/campus that requires condensate to be returned for energy efficiency. But steam heat purchased from a commercial steam heat company in an urban environment is usually dumped to drain to prevent contaminants beyond the steam heat company's control from fouling their boilers.

VISUAL X-C-43



Utility Systems

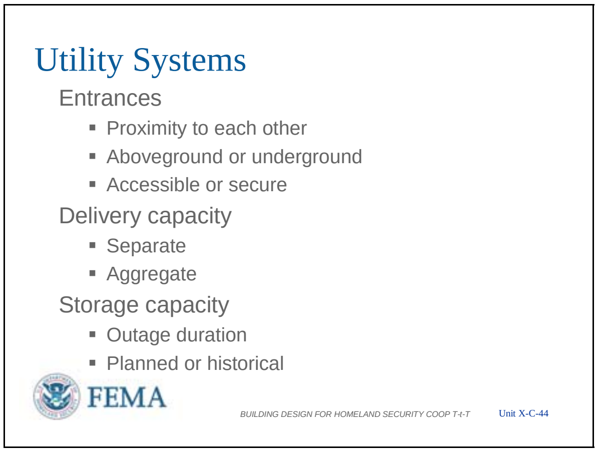
Building Service (cont.)

Thus, anything feeding into and out of the building should be considered due to its impact on the building envelope and building operations if damaged.

For example, water service into a building balances against sewer service to get it out of the building. A sewage lift pump or station that is not on backup power results in raw sewage backing up into the building.

INSTRUCTOR NOTES

VISUAL X-C-44



CONTENT/ACTIVITY

Utility Systems

Service entrances of utilities into buildings take on the following concerns:

- Reduce the number of utility openings, manholes, tunnels, air conditioning ducts, filters, and access panels into the structure. Balance this with having two well separated service entrances for each utility.
- Proximity: How close are the service entrances to each other and can a single event affect more than one utility – for example all utilities entering along the loading dock ramp because the utility room is adjacent or underneath the loading dock.
  - o Locate utility systems away from likely areas of potential attack, such as loading docks, lobbies, and parking areas. The alternative is hardening.
- Above or below ground: Below ground is preferred, but gas meters and pressure regulators, electric meters and transformers, and tankage may be aboveground. By building code gas lines must come above ground before entering a building to prevent gas leaks from following the piping into the building and reaching explosive concentrations in a basement.
- Can someone outside the building access the utility where it enters the building or use it as a way of getting into the building?
  - o Use lockable systems for utility openings and manholes where appropriate. Infrequently used utility covers/manholes can be tack-welded as an inexpensive alternative to locking tamper-resistant covers.

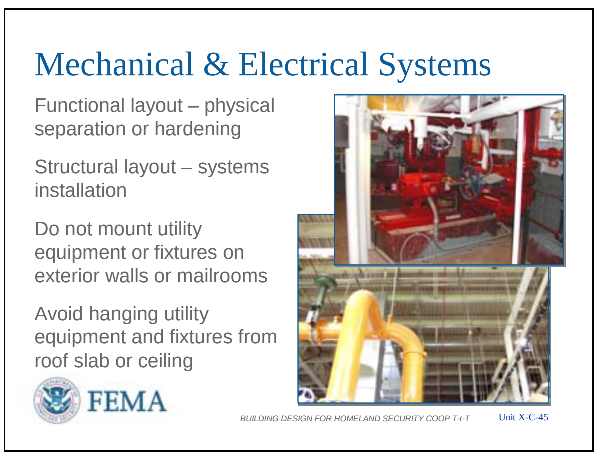
Delivery capacity is an operational consideration before and after an incident:

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Will each service entrance handle 50% of the total building needs or 100% (like hospitals require for electric service). Emergency operations plans should consider all contingencies for losing either or both service entrances for each given utility.

Storage capacity is a concern during:
- Evacuation (i.e., How long will the emergency lighting system continue to operate?)
- Orderly shutdown of a computer system (battery backup for uninterruptible power supply)
- Continued operations (fuel stored for emergency generator use to last as long as historically longest commercial outage or until contingency contracts in place can refuel the generator on an acceptable schedule).

VISUAL X-C-45



Mechanical and Electrical Systems

The major security functions of an electrical are to maintain power to essential building services, provide lighting and surveillance to deter criminal activity, and provide emergency communications.

The primary goal of a mechanical and electrical system after a terrorist attack should be to continue to operate key life safety and evacuations systems.

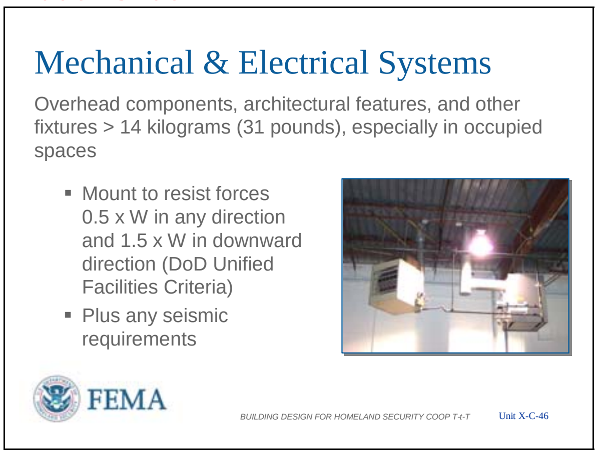
The following suggestions attempt to protect the mechanical and electric systems during an explosive blast event:

- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls, but, when this is unavoidable, mount fixtures on a separate wall at least 6 inches from the exterior wall face.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Avoid suspending plumbing fixtures and piping from the ceiling or roof slab. Remember the upheaval if the blast wave gets inside the building.
  - The roof slab is part of the building envelope.
  - The ceiling is less sturdy than the floor above.
- When the above cannot be done, add ductility, additional supports, and hardening to achieve some level of protection.

VISUAL X-C-46
Hidden Slide



Mechanical and Electrical Systems

Nonstructural Elements

False ceilings, light fixtures, Venetian blinds, ductwork, air conditioning components, and other equipment may become flying debris in the event of an explosion once the building envelope is breached. Marques and other exterior nonstructural elements must also be considered since upward blast pressure will be much greater.

Wherever possible, it is recommended that the design be simplified to limit these hazards. Placing heavy equipment such as air conditioners near the floor rather than the ceiling is one idea; using curtains rather than Venetian blinds, and using exposed duct work as an architectural device are others.
When using seismic requirements added to the above will require about a Seismic Zone 4 (old system) [highest level] design. For example, 30 years ago 2-foot 4-foot light fixtures in drop ceilings required additional support (other than the drop ceiling support) on two opposing corners using 9-gauge wire. Seismic Zone 4 would consider threaded rod on all four corners to satisfy the requirement.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-47

Mechanical and Electrical Systems

Distribution – similar to comments about utility systems previously

- Multiple risers and looping on each floor with isolation valving or switches adds redundancy
- As high voltage and low voltage electricity is separated from communications circuits due to capacitive coupling and fault tolerance situations, other systems should not share the same pipe chases or provide vertical separation to overcome secondary effects of leakage.

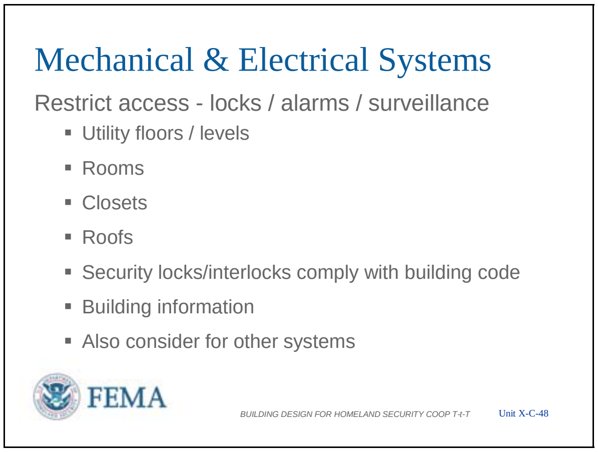
Locations of emergency equipment also figure into redundancy:

- Locate components in less vulnerable areas such as away from loading docks, entrances and parking. Seek 50-foot separation as a minimum.
- Placing emergency switchgear and commercial switchgear in the same room allows one event in either system to affect the other.
- Fuel tanks should be mounted near the emergency generator(s) and be given the same protection as the generator. Separating them puts the fuel distribution at greater risk due to the distance of the separation.
- If an emergency generator cannot be justified, consider running conduits with conductors through a manual transfer switch to a quick disconnect on the outside of the building. A rental generator / company can be prearranged to provide rapid backup power as required without major rewiring. This would be equivalent to a Siamese water connection for adding fire fighting water to a sprinkler system.
- Similarly, placing electric fire pumps and diesel fire pumps side-by-side allows one

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

event to affect both primary and backup systems. The event is not just loss of commercial power.

VISUAL X-C-48

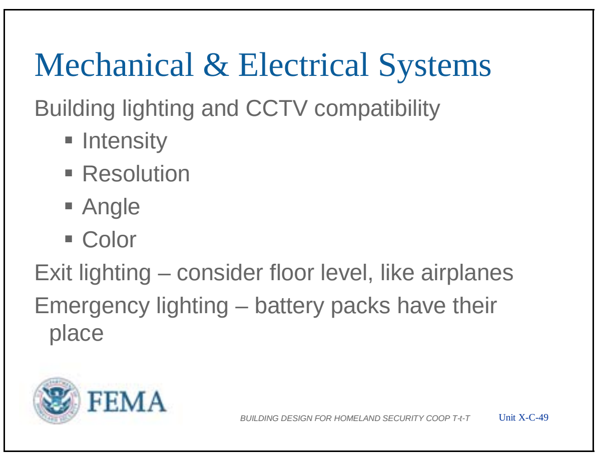


Mechanical and Electrical Systems

Restrict Access

- Physical security for utility rooms, closets, etc., should be implemented to prevent tampering with the systems and to prevent the direct introduction of hazardous materials into heating, ventilating, and air conditioning (HVAC) ducts that distribute air to portion(s) of the building.
- Public access to building roofs should be prevented. Access to the roof may allow entry to the building and access to air intakes and HVAC equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof.
- Access to information on building operations (including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, and emergency operations procedures) should be strictly controlled.

VISUAL X-C-49



Mechanical and Electrical Systems

Closed circuit television/security cameras and building lighting must be worked as a system to ensure compatible operation:

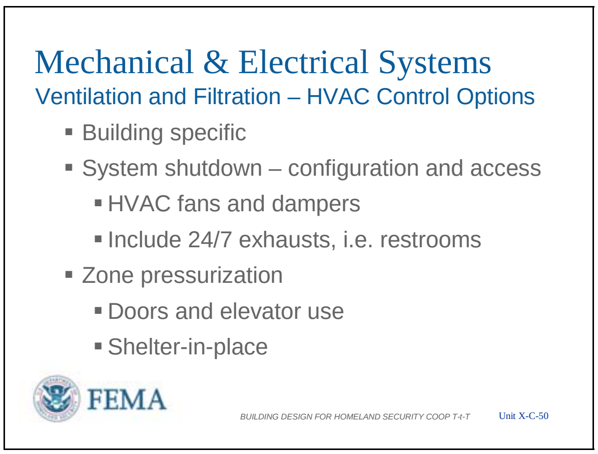
- The intensity, angle, and color of the lighting affect camera resolution, including low-light and infra-red
  - o Detection for response versus identification for police/legal action
- Exit lighting has traditionally been at top of door level shining downward to floor or along halls. After incidents smoke, heat, and toxic fumes are normally lighter than air so traditional exit lighting is obscured. Putting exit lighting at floor level works

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

whether walking upright or crawling.

- Emergency lighting from a distribution system with central batteries and backup generator is one design approach, but distributed emergency lighting with self-contained battery packs along the egress route ensures operation during a wider range of potential incidents. Do not forget restrooms in the emergency lighting scheme.

VISUAL X-C-50



NOTE to instructor: Added egress and CBR considerations

- Provide clear design guidance for entrances, exists, and lighting
- Mobilization of people with disabilities should be carefully considered
- Egress routes should be accessible and well marked
- Egress (stairs and elevators) should take into consideration hardening (structural, fire, water, overpressure, and CBR filtration) and size of potential flows
- Egress should allow dedicated paths for first responders (less likely, unless elevators) or be adequate to accommodate counter flow of emergency responders (more likely if stairs)

Mechanical and Electrical Systems

Ventilation and Filtration – HVAC Control Options

Available options are specific to the building as HVAC equipment and configuration, building functions, continuing operations, and other factors affect what can be done.

- HVAC control may not be appropriate in all emergency situations. Protection from CBR attacks depends upon the design and operation of the HVAC system and the nature of the CBR agent release.
  - Ducted returns (vice using hallways as returns) offer limited access points to introduce a CBR agent. The return vents can be placed in conspicuous locations, reducing the risk of an agent being secretly introduced into the return system.
  - Large buildings usually have multiple HVAC zones, with each zone served by its own air handling unit and duct system.
- Complete system shutdown of all HVAC systems is the simplest initial approach to handle either external or internal releases
  - Since speed is critical, a single shutdown point is desirable, but the larger the system(s) the difficult this becomes.
  - A rapid response may involve closing

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

various dampers, especially those controlling the flow of outdoor air (in the event of an exterior CBR release).

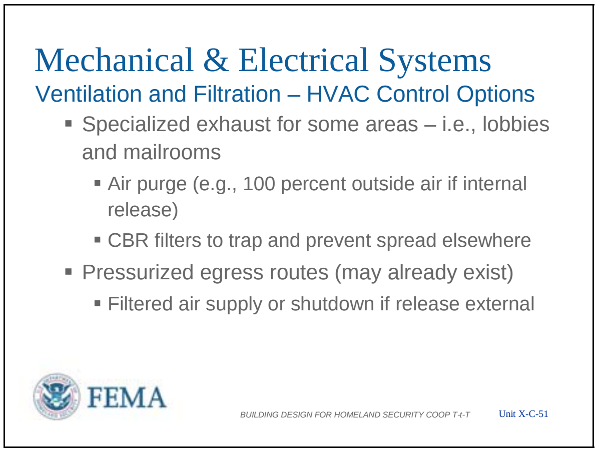
  - Consideration should be given to installing <u>low leakage fast acting dampers</u> to minimize this flow pathway. Fast acting dampers close much faster than in 30 seconds.

- Must include all air handling systems, such as restroom exhausts that run continuously.

- Ensure there is <u>no unintended leakage</u> into or out of the ventilation system – filters sealed to channel all air through them vice taking the path of least resistance and dampers fully functional – <u>Good Maintenance</u>
- If zone pressurization is designed into the system (for fire fighting as an example, where the fire floor is ventilated to remove heat and adjacent areas are overpressurized to keep smoke and gases contained), then realize that opening and closing doors or operating elevators will change the zone pressurization being attempted.
  - Even without zone pressurization, opening and closing doors and operating elevators will affect the flow of air and spread smoke, toxic fumes, and CBR agents within the building.
  - Consider "shelter-in-place" rooms or areas where people can congregate in the event of an outdoor release and, in some cases, indoor releases.
    - Without pressurization the goal is to create areas where outdoor air infiltration is very low.
    - With pressurization requires a filtered air supply from an installed or portable unit with filters suitable for the agent released.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-51



Mechanical and Electrical Systems

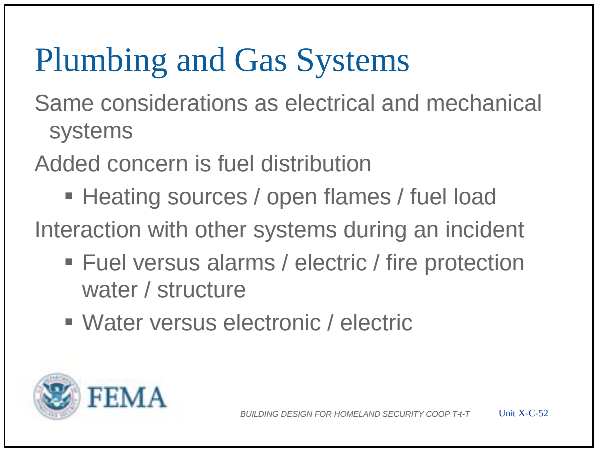
Ventilation and Filtration – HVAC Control Options

- To prevent widespread dispersion of a contaminant released within lobbies, mailrooms, and loading docks, their HVAC systems should be isolated and the areas maintained at a negative pressure relative to the rest of the building, but at positive pressure relative to the outdoors.
  - Air purge is suitable for removal of smoke and toxic fumes from fire or explosive blast
  - If a CBR release, an air purge would not be suitable as it would just spread the agent vice controlling it unless CBR filters are installed on exhaust to trap the agents and prevent spreading them.
  - Another consideration is <u>glazing</u> in these areas.
    - If <u>not hardened</u>, then windows will be blown out during an internal blast which lessens the need for air purge. This is a good design example for a frangible panel that vents pressure and reduces pressure on the walls shared by the rest of the building.
    - If <u>hardened</u>, then smoke and gases are trapped and air purge is beneficial. However, all walls will required additional hardening because of the increased internal blast pressures.
- Egress routes (stairwells) are normally pressurized to prevent smoke from internal fire from entering the stairwells. An external CBR release would be pulled into the stairwells by this system. Thus, either the pressurization system must be turned

INSTRUCTOR NOTES	CONTENT/ACTIVITY

off during an external release or a filtering system must engage to provide clean air to the stairwells.

VISUAL X-C-52



Plumbing and Gas Systems

All systems distributed throughout the building have similar consideration. There are other concerns based upon "What-If" scenarios, such as leaks occurring in plumbing or gas systems.

- Look at the physical relationship between the systems (which also includes utilities as they enter the building)
  - Will a leak in a fuel system reach a heat source and will the fuel distribution system aid in spreading the fire throughout the building?
  - Will leaks from water or fuel systems fall upon electrical systems and equipment?
    - For example, standard underground construction always puts water systems above sewer systems so that a sewer leak will have less chance of contaminating the water system.
    - Additionally, are flammable systems like fuel/natural gas separated from mass notification/communication systems so that an initial fire incident does not disable the mass notification system?

INSTRUCTOR NOTES

VISUAL X-C-53

Fire Alarm Systems

Considerations similar to information and communications systems, but tighter building codes

- Centralized or localized
- Fire alarm panel access for responding fire fighters or fire control center
- Interaction with other building systems
  - Telephone / IT
  - Energy management
  - HVAC controls
- Off-premises reporting and when

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit X-C-53

CONTENT/ACTIVITY

Fire Alarm Systems

Similar concerns as with communications systems to be covered next, but building codes based upon National Fire Protection Association standards are more prescriptive

- First alarm to evacuate, then call the fire department
  - o If localized, alarm bells sound to evacuate the building, then automatically calls fire department
  - o If centralized (hotels for example), a response would verify fire before sounding evacuation and calling fire department from manned location
- Fire alarm panels are normally near main entrances of buildings so first responder fire fighters can determine which zone of the building alarmed if fire location is not obvious
  - o Fire control centers are normally manned and fire department should know where they are located
- Interaction with other systems should confirm wiring of the fire alarm system, whether it is combined with any other system for information flow, and whether or not an alarm activation also initiates actions through other systems, like energy management, SCADA (Supervisory Control and Data Acquisition), or HVAC controls.
- Finally, as explained above, how is off-premises reporting done – direct telephone line to fire department, reporting to a commercial central security/fire company who contacts the fire department, centralized system manned in building which then triggers a call to the fire department or calls 911, autodial to someone else, etc.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-54

NOTE to instructor: The Government Emergency Telecommunications Service (GETS) is a White House-directed emergency phone service provided by the National Communications System (NCS) in the Information Analysis and Infrastructure Protection Division of the Department of Homeland Security.

- GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.
- The result is a cost-effective, easy-to-use emergency telephone service that is accessed through a simple dialing plan and Personal Identification Number (PIN) card verification methodology. It is maintained in a constant state of readiness as a means to overcome network outages through such methods as enhanced routing and priority treatment. See **NOTE** to instructor under Visual X-C-55.

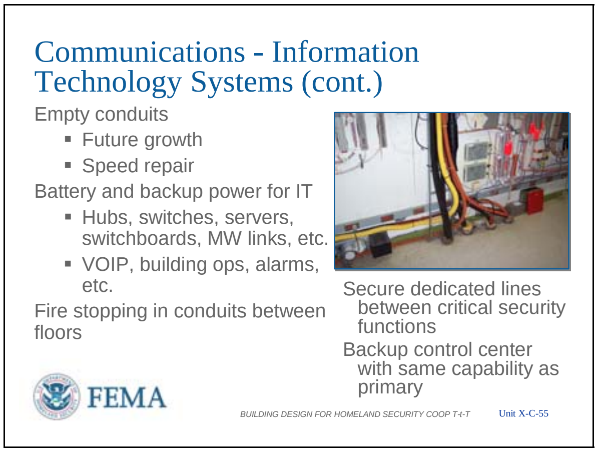
Communications – Information Technology Systems

Distribution considerations are the same as for other systems, especially to ensure some communications capability if an incident affects communication lines

- Redundancy is always a consideration and technology selected has pros and cons
  - Copper easier to tap through electromagnetic signals
  - **Cell phones** get tied up during major incidents, especially analog voice (which locks bandwidth), but walkie-talkie and text features on phones or Blackberrys use packet transmission when bandwidth is available so there is more capability as found during Hurricane Katrina
  - **Handheld radios** have blind spots both in dispersed campuses and high-rise buildings, necessitating use of repeaters or distributed antennas to maintain coverage. Consider a base radio communication system with antenna(s) installed in stairwells, and portable sets distributed on floors.
  - **Alarm and information systems.** Should not be collected and mounted in a single conduit, or even collocated. Circuits to various parts of the building should be installed in at least two directions and/or risers
  - **NOTE**: The red phone shown is a telephone connected to the local telephone company and powered by the telephone company. It is the backup to VOIP phones throughout the campus.
- Mass notification to building occupants can take many approaches, but must ensure system capability or redundancy for the range of potential incidents. Keeping occupants informed as response requirements change is vital to save lives.

INSTRUCTOR NOTES

VISUAL X-C-55



NOTE to instructor: Wireless Priority Service (WPS) allows authorized National Security/Emergency Preparedness personnel to initiate calls during an emergency when cellular networks may be congested.

- WPS gives authorized NS/EP personnel priority cellular access before subscriber who do not have WPS.
- WPS will not preempt calls in progress and does not guarantee call completion.
- In addition, WSP is complementary to, and can be used in conjunction with the Government Emergency Telecommunications Service (GETS) card. This ensures a high probability of call completion in both the landline and cellular portions of the Public Switched Network (PSN).
- Not all wireless providers currently offer the WSP feature.

NOTE to instructor: Two way pagers are also "low tech" solutions during situations that clog communication lines, especially during wide area disasters.

CONTENT/ACTIVITY

Communications – Information Technology Systems (cont.)

The one thing about information is that it is ever expanding, thus future load growth should always be considered, especially extra conduits that assist repairs and allow additional capability as needed.

- These conduits are for future dedicated electrical circuits, updated information systems, and additional security systems. The last being the quickest way to provide reduction in risk.

Note that battery backup and emergency power must be at or link to all distributed equipment in the IT system to keep system functional

- If other capabilities like VOIP (Voice Over Internet Protocol) telephones, building operations, or alarms on IT Systems increases need for the electric backup

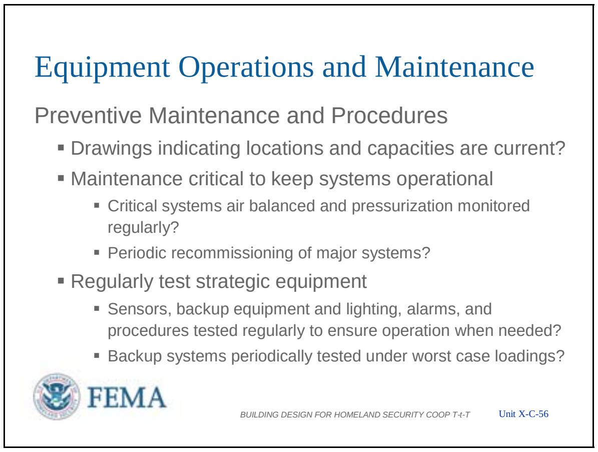
Historically, communications systems have been installed without consideration for other building codes – for example, conduits between floors must have fire stopping installed to prevent spread of fires, fuel leaks, gas leaks, defeat of zone pressurization, or spread of CBR agents and other toxic materials.

Security information and flow of information to building occupants is critical before, during, and after an incident. Dedicated communication lines between security functions – such as central security control and entry control stations keeps information current, especially during deter and detect situations. Control centers for security, fire, and emergency operations may have backup locations depending upon the size of the organization or site. Communications

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

capability should be replicated at the backup site, or if alternative methods are used, staff must be trained for both primary and backup procedures and equipment.

VISUAL X-C-56



Equipment Operations and Maintenance

- Keeping drawings up to date and ensuring capacities meet current needs as functions and infrastructure changes occur are necessary for proper maintenance and operation
- An emergency system that will not function properly when called upon will result in increased damage and casualties
  - In the past, US military installations in a foreign country tested their Class B generator plant (sized to support the complete installation when commercial power lost) at 5:00 am on Sunday morning to avoid inconveniencing people. Class A plants are prime power and used where there is no reliable commercial power. Class C units are also backups but of smaller size and distributed at the critical loads and buildings. One engineer knew that this did not ensure operation when needed and convinced decision makers to run the test during the peak electrical load of the month (units were tested once a month for two hours). It took almost six months of incremental repair before the plant could run for the full 2 hours. Six moths later a country-wide power outage occurred. This installation was the only US installation that stayed fully operational for the whole commercial power outage.
- Bottom line: Preventive maintenance and testing that ensures the systems will work in all required modes, including emergency situations, must be done to ensure proper functioning when they are called upon.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL X-C-57

Equipment Operations and Maintenance

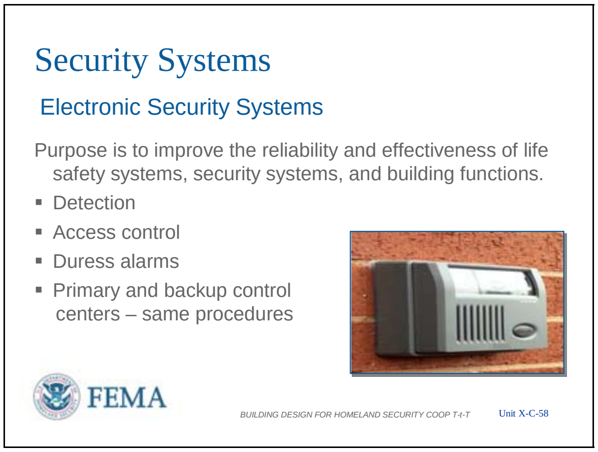
Maintenance Staff Training

Since emergency systems, especially HVAC, are not standard building components, the staff must receive training in how the upgraded mechanical systems are designed to work, how they should be operated, and how they should be maintained and tested.

- A high-rise in Chicago was designed to have all lights burning 24 hours a day in the winter as part of the heating system design. A new manager demanded the lights be turned off and the staff could not explain why so they were turned off. A cold snap hit and the small supplemental boiler in the basement and the lights turned back on took 4 days to bring the building back to desired office temperatures.
- Maintenance and operational staff must have the training in the operational procedures for all potential situations in how the building will be reconfigured, especially for CBR events outside and inside the building.
- Another point based upon experience, is that maintenance staff will be more likely to perform maintenance, repairs, and testing if the equipment is accessible. The more difficult it is to perform these actions the less likely they will be done.
    - Example – steam boiler in penthouse of 3-story building required weekly replenishment of water treatment chemicals. An elevator got the heavy chemicals to the third floor, but to get to the penthouse required winding through offices and then carrying them up a vertical ladder to a roof hatch. The building was originally designed for a location with water that did not need water treatment.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-58



Chapter 3 of FEMA 426 is not a design guide for Electronic Security Systems (ESS). The following criteria are only intended to stress those concepts and practices that warrant special attention to enhance public safety. Consult design guides pertinent to the specific project for detailed information about electronic security. A description of Electronic Security Systems is provided in **Appendix D of FEMA 426.**

Security Systems

Electronic Security Systems

The purpose of electronic security is to improve the reliability and effectiveness of life safety systems, security systems, and building functions. When possible, accommodations should be made for future developments in security systems.

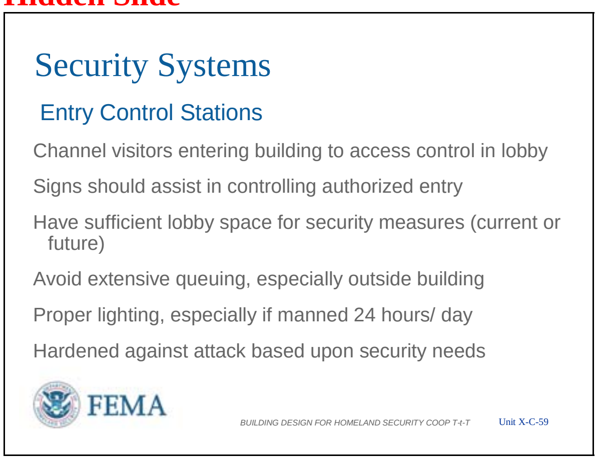
- Basic intrusion detection devices should be provided: magnetic reed switches for interior doors and openings, glass break sensors for windows up to scalable heights, and balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors. Roof intrusion detection should be reviewed.
- A color CCTV surveillance system with recording capability should be provided to view and record activity at the perimeter of the building, particularly at primary entrances and exits.
- Consider duress alarms at Entry Control Stations, where the general public has contact, and other locations as deemed necessary from threat or past history. Also call boxes in parking areas for similar function.
- The Operational Control Center (OCC), Fire Command Center (FCC), and Security Control Center (SCC) may be collocated. If collocated, the chain of command should be carefully pre-planned to ensure the most qualified leadership is in control for specific types of events. Secure information links should be provided between the OCC, FCC, and SCC.
- A Backup Control Center (BCC) should be provided in a different location, such as a manager's or engineer's office. If

feasible, an off-site location should be considered.

- A fully redundant BCC should be installed (this is an alternative to the above).
- An on-site monitoring center should be used during normal business hours and be operational 24 hours. When not manned the monitoring center responsibility can be transferred to an off-site location

These criteria primarily address access control design, including stair and lobby design, because access control must be considered when design concepts for a building are first conceived. Although fewer options are available for modernization projects, some designs can be altered to consider future access control objectives.

VISUAL X-C-59
Hidden Slide



Security Systems

Entry Control Stations

Entry control stations should be provided at main perimeter entrances of the building where security personnel are present (see **Figure 3-12, page 3-48, of FEMA 426**). In addition, entry control stations should be located close to the perimeter entrance to permit people inside the entry control station to maintain constant surveillance over the entrance and its approaches. Note that many of the considerations for entry control stations listed here are appropriate for Site and Layout Design as discussed in **Chapter 2 of FEMA 426**. Additional considerations at entry control stations include:

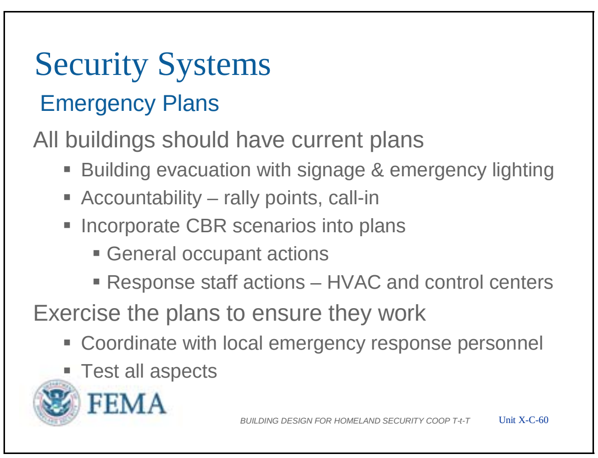
- Channel visitors to access control with appropriate signage to differentiate between visitors and building occupants / tenants
- Additional space is needed for metal

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

detectors and x-ray machines. If not installed initially, allow future space in case they may be installed later.

- Queuing should be limited, i.e. access control should have sufficient throughput to avoid having a high concentration of personnel at the entrance at any time. Queuing that takes the line outside the building should be avoided at all costs.
- Lighting, with CCTV should assist in identification and access control.
- Entry control stations should be hardened against attacks according to the type of threat. The methods of hardening may include:
  - Reinforced concrete or masonry
  - Steel plating
  - Bullet-resistant glass
  - Commercially fabricated, bullet-resistant building components or assemblies
- Entry control stations adjacent to the building but not inside should have appropriate environmental support (heat / air conditioning), lighting, and sufficient glassed area to afford adequate observation for people inside.

VISUAL X-C-60



Security Systems

Emergency Plans

All buildings should have current **emergency plans** to address fire, weather, and other types of emergencies.

In light of past U.S. experiences with anthrax and similar threats, these plans should be updated to consider CBR attack scenarios and the associated procedures. Emergency plans should have procedures for communicating instructions to building occupants, identifying suitable shelter-in-place areas (if they exist), identifying appropriate use and selection of

INSTRUCTOR NOTES	CONTENT/ACTIVITY

personal protective equipment (i.e., clothing, gloves, respirators), and directing emergency evacuations.

Building design should be able to ensure the optimal operation of the emergency plans. The emergency plans should not default to only what can be done after the building is constructed. In other words, like security and homeland defense, emergency planning should be an up-front design consideration that gets incorporated into the planning, budgeting, and design of the building.

Note that bomb threats have been used in the past by terrorists to evaluate evacuation procedures and determine where the evacuees congregate after leaving the building. Consider multiple rally points (A, B, and C) and vary their use so that a pattern cannot be determined by terrorist surveillance.

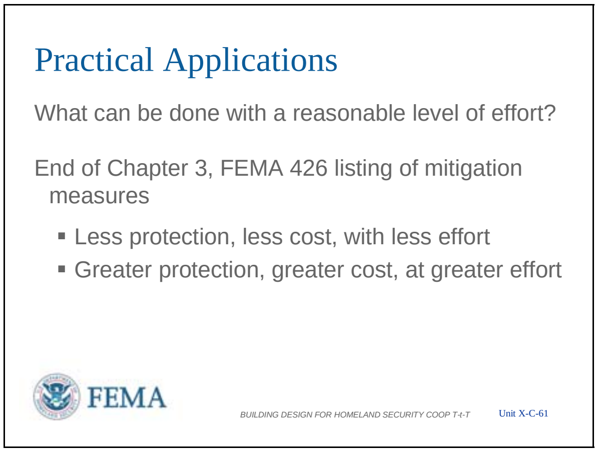
Then the plans must be tested to ensure they work in all situations, that what is written can actually be done, especially at the speed required, and that the plans and equipment operation work in agreement.

Note that walking egress routes are not always down a single stairwell, especially in high-rise building as in the World Trade Center Complex. Recommend exercising an annual evacuation exercise to ensure most people know the egress routes (primary and alternate) and can negotiate them in a speedy manner. Signage and lighting along the whole route should also be evaluated at the same time.

Additionally, all security locking arrangements on doors used for egress must comply with requirements of the National Fire Protection Association (NFPA) 101, Life Safety Code.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-C-61



Direct students to **Table 2-1 in FEMA 426** and arrow listing on **pages 3-51 and 3-52 of FEMA 426.**

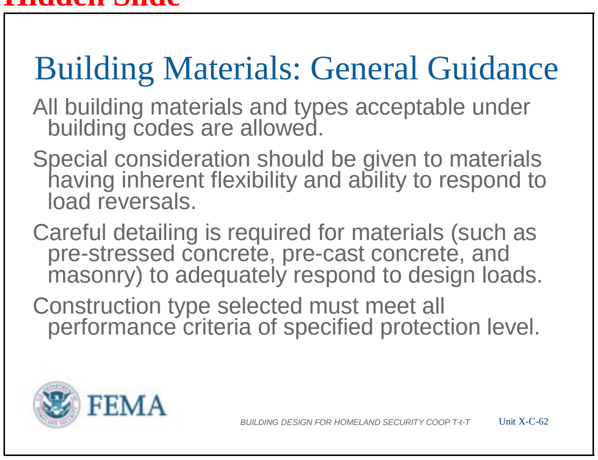
Practical Applications

What can be done with a reasonable level of effort?

Consult **Table 2-1, page 2-54, of FEMA 426** to understand the benefit of various mitigation efforts against a range of terrorist tactics.

There is a range of FEMA 426 mitigation efforts at a range of cost. Consult **pages 3-51 and 3-52 of FEMA 426** to see the range of relative costs for most situations.

VISUAL X-C-62
Hidden Slide

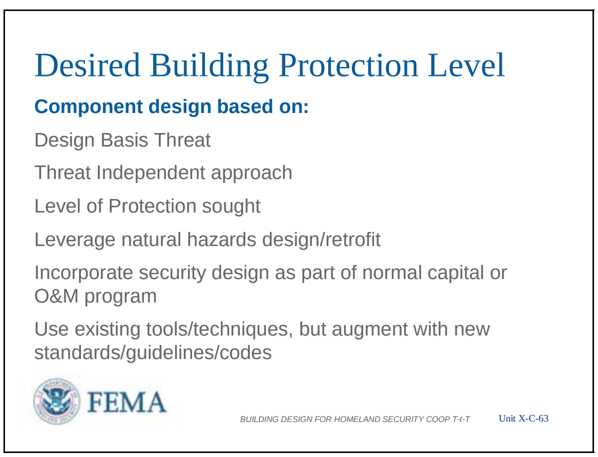


Building Materials: General Guidance

- All building materials and types acceptable under model building codes are allowed (except unreinforced masonry – brick and/or CMU (concrete masonry unit) – concrete block.
- Special consideration should be given to materials that have inherent flexibility and that are better able to respond to load reversals (i.e., cast in place reinforced concrete and steel construction).
- Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry (brick and concrete masonry unit) to adequately respond to the design loads. Even calling out seismic connections may not be adequate as the workforce may not be familiar with the changes from their norm; thus detailing is very important.
  - For example, aluminum wiring is not used in homes in the US because copper trained electricians over-

INSTRUCTOR NOTES

VISUAL X-C-63



Establishing the design basis threat early in the design cycle reduces cost, has synergies with other requirements – seismic and wind, and should never be an afterthought of the design. Even for a low threat, there is value

CONTENT/ACTIVITY

torqued the connections, causing cold flow, loose connections, and fires. Great Britain took path to put copper on the outside of aluminum, taking advantage of the less expensive aluminum without getting the cold flow problem.

  - Another example, plastic water pipe initially installed by copper-trained plumbers were not twisted 90 degrees to spread the glue as this was not needed when soldering copper. Imperfections in the plastic would scrape the glue away resulting in leaks. Plumbers now know this procedure and we still use plastic water piping.

- The construction type selected must meet all performance criteria of the specified level of protection.
- The designer must bear in mind that the design approaches are, at times, in conflict. These conflicts must be worked out on a case by case basis.

Desired Building Protection Level

The assessment process to this point should determine the level of protection sought for the building structure based upon the threat / hazard specific to the facility. Explosive blast threats usually govern building structural design for high risk buildings.

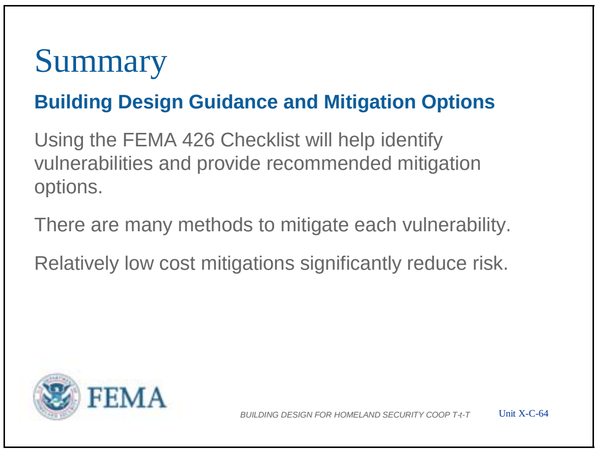
Some design approaches are threat independent, such as progressive collapse. Other approaches depend upon an identified Design Basis Threat. The design basis threat is the terrorism hazard equivalent to the natural hazards design basis which is based upon recorded history, measurement methods to determine the magnitude of the hazard and have been established as building codes based on the weather and geological conditions of the locality.

INSTRUCTOR NOTES

in providing certain minimum features to the site and building design. This allows adjustment to the level of protection if the level of threat changes. This is the current philosophy of the Department of Defense.

Even if no design changes result, the understanding in going through the assessment process, especially in the data collection and identifying Points of Contact, is beneficial if future man-made hazards threaten or occur.

VISUAL X-C-64



CONTENT/ACTIVITY

Whenever there are projects to accomplish in a building, seek to leverage natural hazard upgrades, energy conservation upgrades, and other capital improvement or O&M (Operations and Maintenance) work to achieve synergies at less cost to achieve HVAC upgrades and building hardening.

In every design situation, the intent is to seek a balance between all the different requirements to include in the design (e.g., antiterrorism, energy conservation, building code, seismic, wind, snow loading, handicap access, adjacent architecture, etc.).

Summary

To summarize:

This unit provides a foundation for a systematic approach to assessing the vulnerabilities of a building to manmade hazards.

The **Building Vulnerability Assessment Checklist in FEMA 426** can provide an excellent framework for the identification of mitigation options that will, over time, significantly reduce the vulnerability of a building to manmade hazards.

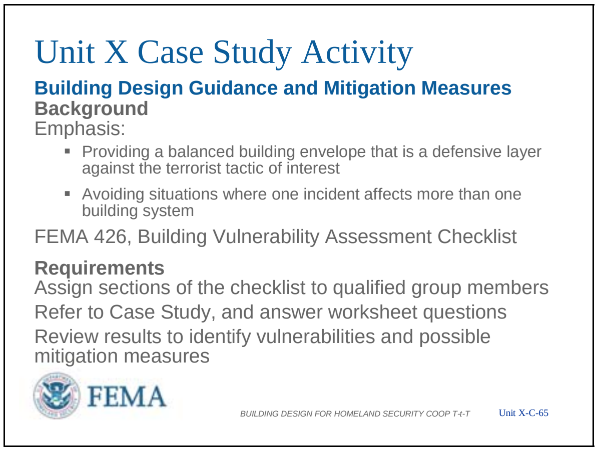
Note that there are many different techniques to mitigate each vulnerability. They have different costs and may increase, reduce, or have no effect on risk for other tactics. Thus, each mitigation measure needs to be compared to every threat / hazard tactic for the building particulars.

Antiterrorism assessment teams that have been operating over 5 years indicate that historically about 80 percent of mitigation recommendations are low cost /no cost

INSTRUCTOR NOTES	CONTENT/ACTIVITY

planning and procedural changes.

VISUAL X-C-65



Refer participants to **FEMA 426**, the Unit X 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 45 minutes, reconvene the class and facilitate group reporting. Take 15 minutes to review group results.

There are <u>25 questions</u> to answer by the team and then confer. With an average of 7 team members this means each member answers about 4 questions or about <u>7 minutes per question</u> during their 30 minutes of research.

Student Activity

The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for vulnerability assessment of an existing building or a preliminary design.

The checklist includes questions that determine if critical systems will continue to function to enhance deterrence, detection, denial, and damage limitation, and emergency systems function during a threat or hazard situation.

Activity Requirements

- Continue working is small groups.
- Assign sections of the checklist to the group members who are most knowledgeable and qualified to perform an assessment of the assigned area. There are 49 questions so that with 7 students (working group size sought), each student would need to answer 7 questions in about 30 minutes (4-5 minutes per question) leaving 15 minutes to discuss results as a group.
- Refer to the Case Study to determine answers to the worksheet questions.
- Then review results as a team to identify vulnerabilities and possible mitigation measures.

Take 45 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

Unit XI will cover Electronic Security Systems.

UNIT X (C) CASE STUDY ACTIVITY: BUILDING DESIGN GUIDANCE (COOP Version)

In this student activity, the emphasis is identifying vulnerabilities in the building design. The **Building Vulnerability Assessment Checklist in FEMA 426 (Table 1-22, pages 1-46 to 1-93)** provides a tool for vulnerability assessment of the proposed and existing sites and buildings.

Requirements

Assign sections of the checklist to group members who are most knowledgeable and qualified to perform an assessment of the assigned area. Refer to the Appendix C Case Study to determine answers to the questions. Then review results as a team to identify vulnerabilities and possible mitigation measures.

Activity # 1: Complete the selected vulnerability checklist questions in the following Vulnerability Questions table.

> **Note**: There are **25 questions** below (**9** in Section 2, **4** in Section 3, **1** in Section 4, **3** in Section 6, **3** in Section 8, **3** in Section 9, and **2** in Section 10), so it is recommended that the team split up the questions among themselves taking 3-5 questions each and review the Appendix C Case Study for answers. Apportion the available time for gathering the answers and then provide each other the answers while performing the actions below.

Activity # 2: Upon completion of the questions refer back to the vulnerability ratings determined in the Unit IV (C) Student Activity. Based on this more detailed analysis, decide if any vulnerability rating needs adjustment. Adjust the Risk Matrix poster accordingly for any changes in vulnerability rating.

Activity # 3: Select mitigation measures to reduce vulnerability and associated risk from the building perspective. Concentrate on the three highest risk ratings on the Risk Matrix poster as adjusted by Activity # 2. Use the Building Design Mitigation Measures table found at the end of this unit to capture this information.

Activity # 4: Consider the mitigation measures of Activity #3 to be installed, estimate the new vulnerability ratings as if these measures were in place, and calculate the new risk ratings. Capture your information in the Building Design Mitigation Measures table.

Section	Vulnerability Question	Guidance	Observations
2	**Architectural**		
2.7	Is access control provided through main entrance points for employees and visitors? (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***Visitor access control is handled in the lobby by the receptionist, who signs the visitors in and contacts staff to provide escort. Employees use electronic access control to enter the building.*** ***Access control at other companies within the complex is unknown.***
2.9	Is access to elevators distinguished as to those that are designated only for employees and visitors?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***No elevators in building.***
2.10	Do public and employee entrances include space for possible future installation of access control and screening equipment?	These include walk-through metal detectors and x-ray devices, identification check, electronic access card, search stations, and turnstiles. Reference: *GSA PBS-P100*	***Yes, lobby / reception area within building could accommodate space-saving screening equipment. Interior office space also has adequate room for such equipment.***
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; Uninterruptible Power Supply (UPS) systems controlling critical functions; Main refrigeration and ventilation systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should	***Electrical service is provided through two buried transmission lines from two separate pad-mounted transformers outside the building near the rear loading dock. Emergency power is provided by a single diesel generator, located in a shed in the rear parking lot, also near the loading dock. The generator has a 250-gallon day tank, maintained at 80 percent capacity. The 2,000-gallon main tank is buried under the parking lot, near the generator.*** ***The batteries to support the UPS are in a small room next to the UPS room.***

Section	Vulnerability Question	Guidance	Observations
		be located away from potential attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. Reference: *GSA PBS-P100*	***Natural gas enters the building through two meters under the loading dock staircase and goes overhead to the mechanical and electrical (M&E) room at the building's southwest corner.*** ***The Communications Center has an outside wall as does the Electrical/Mechanical Room. Both can be reached from the rear parking area.*** ***Due to the size of the building, separation of critical assets away from higher threat areas is very limited.*** ***Most of the critical utilities are either in the rear parking area or near the loading dock or both.*** ***None of the critical assets has any hardening or special considerations.***
2.16	Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building. Reference: *GSA PBS-P100*	***People are located along the exterior wall at the front of the building. The Secure Space, Secure Office Space, and Conference Room have the best interior space location – not on an exterior wall. The remaining office space acts as the buffer between the critical functions in the back and the public area of the building at the main entrance.*** ***M&E room is located on an exterior wall.*** ***The Business Center can be considered a public use area, with some restrictions. The secure areas are separated from the public areas by walls and doors with access controls.***

Section	Vulnerability Question	Guidance	Observations
2.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?	Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against explosive blast. Consider a 50-foot separation distance in all directions. Reference: *GSA PBS-P100*	***No, the loading dock connects directly into interior space, critical functions, and infrastructure. A commercial power transformer, the natural gas meters, and the M&E rooms are within 50 feet of the loading dock.*** ***The Communications Center is separated from the loading dock as is the telephone and telecommunications lines.***
2.20	Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets? Is the mailroom located near the loading dock?	The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief. By separating the mailroom and the loading dock, the collateral damage of an incident at one has less impact upon the other. However, this may be the preferred mailroom location. Off-site screening stations or a separate delivery processing building on site may be cost-effective, particularly if several buildings may share one mailroom. A separate delivery processing building reduces risk and simplifies protection measures. Reference: *GSA PBS-P100*	***CI/BC has no mail room. Incoming mail is normally processed by the receptionist in the foyer inside the front door. Large packages are delivered to the loading dock.*** ***The foyer, where mail is delivered, is of standard office construction. Explosive blast inside the foyer would affect exterior walls (glazing) and interior walls (gypsum board on metal studs) about equally.***
2.23	Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur? Are stairways maintained with positive pressure or are there other smoke control systems?	Consider designing stairs so that they discharge into other than lobbies, parking, or loading areas. Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc. out of the stairway. Pressurize exit stairways in accordance with the National Model Building Code.	***Stairways are located in the interior of the building, away from the perimeter walls. They are part of the steel mezzanine design and are towards the front of the building. Multiple exits are located around the building and from both the front and rear. Emergency stairways from mezzanine are located on opposite ends of the non-Information Division spaces***

Section	Vulnerability Question	Guidance	Observations
		Reference: *GSA PBS-P100 and CDC/NIOSH, Pub 2002-139*	***Stairways are open and not designed with any fire protection features, such as a positive pressure system.***
2.26	Are emergency systems located away from high-risk areas?	The intent is to keep the emergency systems out of harm's way, such that one incident takes out all capability – both the regular systems and their backups. Reference: *FEMA 386-7*	***The high risk areas are the front entrance and the rear loading dock. Emergency / backup generator is located over 50 feet away from main power supply lines, loading dock, and M&E room. UPS is located inside the building's high bay area, but probably within 50 feet of the loading dock.***
3	**Structural Systems**		
3.1	What type of construction? What type of concrete and reinforcing steel? What type of steel? What type of foundation?	The type of construction provides an indication of the robustness to abnormal loading and load reversals. A reinforced concrete moment-resisting frame provides greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or unreinforced. A rapid screening process developed by FEMA for assessing structural hazards identifies the following types of construction with a structural score ranging from 1.0 to 8.5. A higher score indicates a greater capacity to sustain load reversals. Wood buildings of all types - 4.5 to 8.5 Steel moment-resisting frames - 3.5 to 4.5 Braced steel frames - 2.5 to 3.0 Light metal buildings - 5.5 to 6.5	***Located in a suburban office complex, the CI/BC office building comprises a 19,000-square foot main floor for offices and computers, and a 3,300-square foot executive mezzanine (a second floor over part of the office).*** ***The building is an office building of standard construction.*** ***The walls are made of concrete blocks (CMU-concrete masonry units) with a brick veneer on the outside. Steel framework supports the structure, and exposed interior columns are enclosed in gypsum wallboard. The roof is a metal deck with gravel on top and insulation underneath. It is slightly angled to allow water to drain. The roof overhangs the front entrance by 8 feet. This provides a covered area for employees to stay dry on rainy days. Cylindrical columns support the overhang.***

Section	Vulnerability Question	Guidance	Observations
		Steel frames with cast-in-place concrete shear walls - 3.5 to 4.5 Steel frames with unreinforced masonry infill walls - 1.5 to 3.0 Concrete moment-resisting frames - 2.0 to 4.0 Concrete shear wall buildings - 3.0 to 4.0 Concrete frames with unreinforced masonry infill walls - 1.5 to 3.0 Tilt-up buildings - 2.0 to 3.5 Precast concrete frame buildings - 1.5 to 2.5 Reinforced masonry - 3.0 to 4.0 Unreinforced masonry - 1.0 to 2.5 References: *FEMA 154 and Physical Security Assessment for the Department of Veterans Affairs Facilities*	
3.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?	The extent of damage to the structure and exterior wall systems from the bomb threat may be related to a protection level. The following is for new buildings: Level of Protection Below Antiterrorism Standards - Severe damage. Frame collapse/massive destruction. Little left standing. Doors and windows fail and result in lethal hazards. Majority of personnel suffer fatalities. Very Low Level Protection - Heavy damage. Onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards. Majority of	***The standard construction techniques used to build the site CI/BC occupies do not create buildings that withstand explosive blasts. Terrorist threat was not a part of design consideration.***

Section	Vulnerability Question	Guidance	Observations
		personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities. Low Level of Protection - Moderate damage, unrepairable. Major deformation of non-structural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely. Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards. Majority of personnel suffer significant injuries. There may be a few (<10 percent) fatalities. Medium Level Protection - Minor damage, repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable. Some minor injuries, but fatalities are unlikely. High Level Protection - Minimal damage, repairable. No permanent deformation of primary and secondary structural members or non-structural elements. Glazing will not break. Doors will be reusable. Only superficial injuries are likely. Reference: *DoD UFC 4-010-01*	
3.6	Is the structure vulnerable to progressive collapse?	Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major	***Since the CI/BC building is a one story building with a mezzanine, progressive collapse is not a great concern. Loss of a perimeter***

Section	Vulnerability Question	Guidance	Observations
	Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse? In the event of an internal explosion in an uncontrolled public ground floor area, does the design prevent progressive collapse due to the loss of one primary column? Do architectural or structural features provide a minimum 6-inch stand-off to the internal columns (primary vertical load carrying members)? Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?	structural element or the system's ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted. Reference: *GSA PBS-P100*	***column would result in localized collapse as would loss of a column holding up the mezzanine.***
3.10	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	Design the floor of the loading dock for blast resistance if the area below is occupied or contains critical utilities. Reference: *GSA PBS-P100*	***The loading dock is the weakest part of the exterior rear wall. There are no hardened walls between the loading dock and the rest of the building as the plan shows only standard gypboard and metal stud walls.*** ***Thus the loading dock will not limit any damage into the building and anything occurring on the loading***

Section	Vulnerability Question	Guidance	Observations
			dock will directly affect the building interior. ***Fortunately, the vehicles only back up to the loading dock and the vehicles do not enter the building.***
4	**Building Envelope**		
4.2	Is there less than 40 percent fenestration per structural bay? Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.) Do the glazing systems with a ½-inch (¾-inch is better) bite contain an application of structural silicone? Is the glazing laminated or is it protected with an anti-shatter (fragment retention) film? If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?	The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40 percent of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows; an architect may favor window curtain walls; building codes require so much fenestration per square footage of floor area; fire codes require a prescribed window opening area if the window is a designated escape route; and the building owner has cost concerns. Ideally, an owner would want 100 percent of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat– weapon size at the expected stand-off distance). However, economics and geometry may allow 80 percent to 90 percent due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher).	***All windows are in the office space area of the building (complete in the front and half of one side). In that area the fenestration is more than 40%.*** ***Fenster is German for window.*** ***The window system is standard commercial construction and thus, the glass, framing, and anchorage are expected to be insufficient for the design basis threat at the available stand-off. One benefit is that there are windows only on two sides of the building.***

Section	Vulnerability Question	Guidance	Observations
		Reference: *GSA PBS-P100*	
6	**Mechanical Systems (HVAC and CBR)**		
6.1	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?	Air intakes should be located on the roof or as high as possible. Otherwise secure within CPTED-compliant fencing or enclosure. The fencing or enclosure should have a sloped roof to prevent the throwing of anything into the enclosure near the intakes. Reference: *GSA PBS-P100 states that air intakes should be on the fourth floor or higher and, on buildings with three floors or less, they should be on the roof or as high as practical. Locating intakes high on a wall is preferred over a roof location.* Reference: *DoD UFC 4-010-01 states that, for all new inhabited buildings covered by FEMA 426, all air intakes should be located at least 3 meters (10 feet) above the ground.* Reference: *CDC/NIOSH, Pub 2002-139 states: "An extension height of 12 feet (3.7 m) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes."* Reference*: LBNL Pub 51959: Exhausts are also a concern during an outdoor release, especially if exhaust fans are not*	***Outside air is brought in through a vent in the wall. The vent is alarmed to prevent intruder access.*** ***A screened exhaust duct is on the roof.***

Section	Vulnerability Question	Guidance	Observations
		in continuous operation, due to wind effects and chimney effects (air movement due to differential temperature).	
6.3	Are there multiple air intake locations?	Single air intakes may feed several air handling units. Indicate if the air intakes are localized or separated. Installing low-leakage dampers is one way to provide the system separation when necessary. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***No, there is only one air intake.***
6.4	What are the types of air filtration? Include the efficiency and number of filter modules for each of the main air handling systems. Is there any collective protection for chemical, biological, and radiological contamination designed into the building?	MERV – Minimum Efficiency Reporting Value HEPA – High Efficiency Particulate Air Activated charcoal for gases Ultraviolet C for biologicals Consider mix of approaches for optimum protection and cost-effectiveness. Reference: *CDC/NIOSH Pub 2002-139*	***The air used to heat or cool the building is filtered in the HVAC room using standard industrial grade MERV 8 filters.*** ***There is no CBR protection designed into the building.***
8	**Electrical Systems**		
8.1	Are there any transformers or switchgears located outside the building or accessible from the building exterior? Are they vulnerable to public access? Are they secured?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***The two 12.47KV feeders lead to two separate transformers outside the building, one near the north side by the loading dock, and the other near the south side by the M&E room.*** ***These transformers are in the rear parking lot, accessible to the public and secured only by a heavy duty lock.***
8.4	Are critical electrical systems collocated with other building systems?	Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers.	***Yes, the electrical system is located adjacent to the main telecommunication and server closet. The HVAC***

Section	Vulnerability Question	Guidance	Observations
	Are critical electrical systems located in areas outside of secured electrical areas? Is security system wiring located separately from electrical and other service systems?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***room is also located adjacent to the electrical distribution room.*** ***Commercial and backup switchgear are both in the M&E room. Wiring is run as inexpensively as possible to minimize rental costs, which means in same pipe chases or adjacent conduit.***
8.6	Does emergency backup power exist for all areas within the building or for critical areas only? How is the emergency power distributed? Is the emergency power system independent from the normal electrical service, particularly in critical areas?	There should be no single critical node that allows both the normal electrical service and the emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear are the initial concerns. Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible. Reference: *GSA PBS-P100*	***Yes, emergency backup power exists and can be routed to all areas of the building. The automatic transfer switch in the M&E room is a single point vulnerability in the system.*** ***Critical computer systems are backed up by an UPS (uninterruptible power supply) that is maintained separately from the site's generator back-up power.*** ***All individual computers / monitors have small (~750va) UPSs.***
9	**Fire Alarm Systems**		
9.1	Is the building fire alarm system centralized or localized? How are alarms made known, both locally and centrally? Are critical documents and control systems located in a secure yet accessible location?	Fire alarm systems must first warn building occupants to evacuate for life safety. Then they must inform the responding agency to dispatch fire equipment and personnel. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***The building fire alarm system is centralized. The fire alarm is routed over telephone lines directly to the fire department. No intermediate monitoring agency is required for notification. An intermediate monitoring system is only used for the security alarm. However, this intermediate security monitoring agency also monitors the fire alarm system and contacts the fire department as a backup to the directly connected fire alarm.***

Section	Vulnerability Question	Guidance	Observations
9.2	Where are the fire alarm panels located? Do they allow access to unauthorized personnel?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***The fire alarm panels are located in the building portion adjacent to CI/BC. The CI/BC security manager has a key to that part of the building for access to the fire alarm panels. However, the panels are accessible to the occupants / tenants of that building portion.***
9.3	Is the fire alarm system standalone or integrated with other functions such as security and environmental or building management systems? What is the interface?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***The fire alarm system is standalone and separate from the security system. The system uses the telephone circuits to place a call to the local fire department.***
10	**Communications and IT Systems**		
10.5	Are there redundant communications systems available?	Critical areas should be supplied with multiple or redundant means of communications. Power outage phones can provide redundancy as they connect directly to the local commercial telephone switch off site and not through the building telephone switch in the main telephone distribution room. A base radio communication system with antenna can be installed in stairwells, and portable sets distributed to floors. References: *GSA PBS-P100 and FEMA 386-7*	***No, there are no installed redundant communication systems available as part of any building system. The only redundant communications are cell phones which operate throughout the building.***
10.15	Is there a mass notification system that reaches all building occupants? (public address, pager, cell phone, computer override, etc.)	Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident if there is redundancy and power. Reference: *DoD UFC 4-010-01*	***The telephone system has a building-wide announcing feature that can be activated by pressing one button at any phone. It reaches all users within audible distance of a phone.*** ***This system will continue to***

	Will one or more of these systems be operational under hazard conditions? (UPS, emergency power)		***operate on the UPS and/or backup generator power.***

Building Design Mitigation Measures
(COOP Version)

NOTE: There is too much variance in student answers compared to a "school solution" to populate this table with information that can be compared to the various team answers.

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

This page intentionally left blank

Unit XI (C)

COURSE TITLE Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer **TIME** 45 minutes

UNIT TITLE Electronic Security Systems

OBJECTIVES

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

SCOPE

The following topics will be covered in this unit:

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

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*:
   a. Pages 3-46 to 3-50
   b. Appendix D
   c. Security Systems and Security Master Plan sections of Building Vulnerability Checklist, pages 1-81 and 1-92
2. Case Study – Appendix C: COOP, Cooperville Information / Business Center
3. Student Manual, Unit XI (C) (info only – do not list in SM)
4. Unit XI (C) visuals (info only – do not list in SM)

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*(one per student)

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

UNIT XI (C) OUTLINE

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, this unit comes after Units IX and X where Local Area content is most easily inserted and this instruction unit supplements Units IX and X. Then, as appropriate, locally oriented discussion can be inserted, especially if done in conjunction with the Case Study.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will complete their familiarization with the Case Study materials. The Case Study is a risk assessment and analysis of mitigation options and strategies for a typical commercial office building located in a mixed urban-suburban environment business park. The assessment uses the DoD Antiterrorism Standards and the GSA Interagency Security

Criteria to determine Levels of Protection and identify specific vulnerabilities. Mitigation options and strategies will use the concepts provided in **FEMA 426** and other FEMA publications related to risk management, emergency planning, and disaster recovery.

- Refer students to their Student Manuals for worksheets and activities.
- Direct students to the appropriate page (Unit #) in the Student Manual.
- Instruct the students to read the activity instructions found in the Student Manual.
- 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. After each response 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, provide the "school solution" and move on.
- For this activity, the assessment of the building's security systems in greater depth may prompt the groups to adjust the vulnerability ratings in their Risk Matrix, with resultant changes to risk ratings.
- If time is short, simply provide the "school solution" and ask for questions. Do not end the activity without ensuring that students know if their answers are correct or at least on the right track.
- Ask for and answer questions.

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

(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

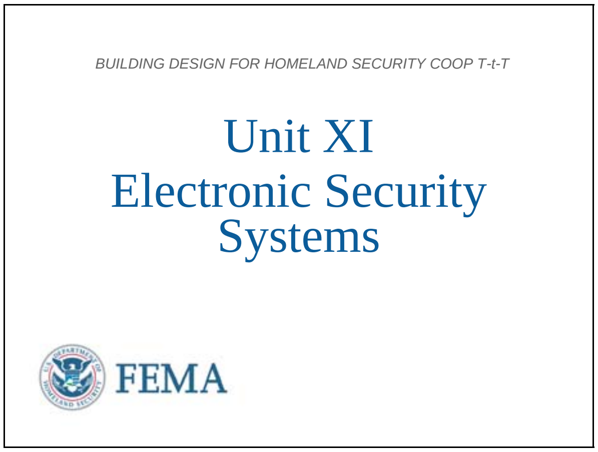
(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

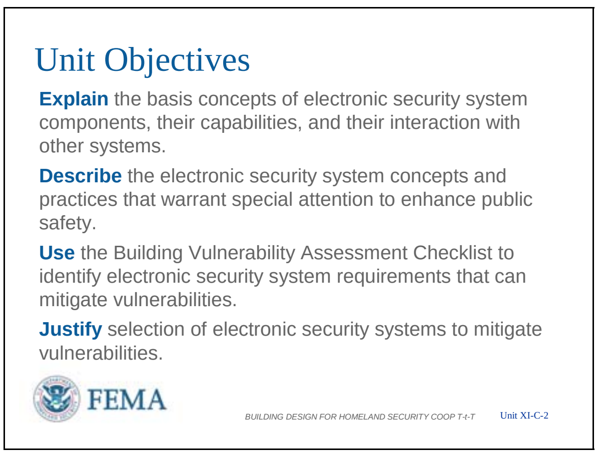
VISUAL XI-C-1



Introduction and Unit Overview

This is Unit XI Electronic Security Systems (ESS). This unit will describe the types of sensors, concepts of operation of electronic security systems, and terminology used in the industry.

VISUAL XI-C-2



Unit Objectives

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

1. Explain the basis concepts of electronic security system components, their capabilities, and their interaction with other systems.
2. Describe the electronic security system concepts and practices that warrant special attention to enhance public safety.
3. Use the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** to identify electronic security system requirements that are needed to mitigate vulnerabilities.
4. Justify selection of electronic security systems to mitigate vulnerabilities.

INSTRUCTOR NOTES

VISUAL XI-C-3

Electronic Security System (ESS) Concepts

- Basic concepts of site security systems
- Use of ESS
- General ESS Description
- ESS Design Considerations

FEMA BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit XI-C-3

CONTENT/ACTIVITY

Electronic Security Systems Concepts

The **Building Vulnerability Assessment Checklist**, **Section 12 (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** can be used for the assessment of security systems. Security systems historically have been designed, installed, serviced, and monitored by physical security companies, typically after the completion of the building. New Internet and wireless technologies have significantly changed the way in which security systems are designed and now incorporation of security system design and processes should begin at the earliest stages of design or renovation. An electronic security system is the physical implementation of the elements of the Layers of Defense:

- Deter
- Detect
- Deny
- Devalue

In this unit, the student should have an appreciation for:

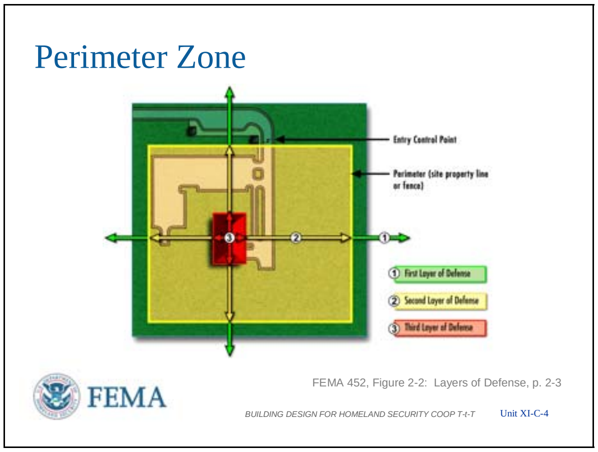
- Basic concepts of ESS
- Use of ESS
- General ESS Description
- ESS Design Considerations

Fundamental objective:
Provide appropriate, effective, and economical protective design for assets.

Approach:
Coordinated effort between security, law enforcement, and engineering communities.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-C-4



Perimeter Zone

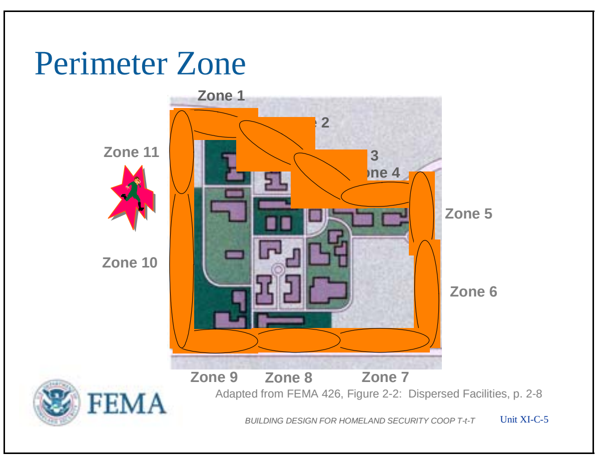
The protection of a facility is designed with layers of defense, detection, and response. Before we discuss security systems, we need to review several basic concepts:

- A protected area's perimeter is usually defined by an enclosing wall or fence, or a natural barrier, such as water. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined.

Perimeter Zone and Layers of Defense

- First layer of defense is from the perimeter outward (either fenceline or owned property).
- Second layer of defense is between the perimeter and the building.
- Third layer of defense is the building envelope.
- A fourth layer of defense may be a room inside the building.

VISUAL XI-C-5



Perimeter Layout and Zoning Sensors

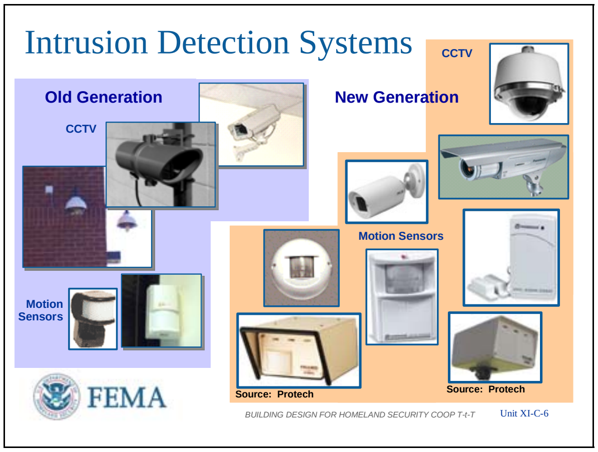
- After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, the existing terrain, and the operational activities along the perimeter.
- The exterior and interior Intrusion and Detection Systems should be configured as layers of unbroken rings concentrically surrounding the asset. These rings should correspond to defensive layers that constitute the delay system. The first detection layer is located at the outermost defensive layer necessary to provide the required delay. Detection layers can be on

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

a defensive layer, in the area between two defensive layers, or on the asset itself, depending on the delay required.

- If an alarm occurs in a specific zone, the operator can readily determine its approximate location by referring to a map of the perimeter.

VISUAL XI-C-6



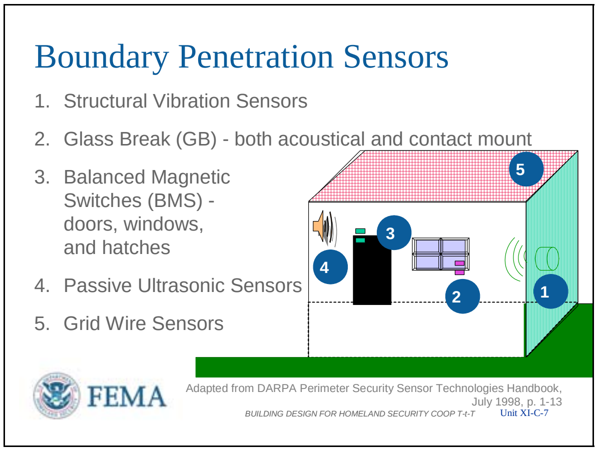
This slide shows old generation and new generation CCTV cameras and motion detectors.

Intrusion Detection Systems

There are a number of different sensor technologies:

- Boundary Penetration Sensors
- Volumetric Motion Sensors
- Exterior Intrusion Detection Sensors
- Fence Sensors
- Buried Line Sensors
- Microwave Sensors
- Infrared Sensors
- Video Motion Sensors

VISUAL XI-C-7



Boundary Penetration Sensors

- Structural Vibration Sensors
- Glass Breaking Sensors
- Balanced Magnetic Switches
- Passive Ultrasonic Sensors
- Grid Wire Sensors

Structural vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives, (subterranean digging) or employing other forcible methods of entry.

Glass breaking sensors detect the breaking

INSTRUCTOR NOTES	CONTENT/ACTIVITY

of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. (This type of sensor should not be used without another sensor type).

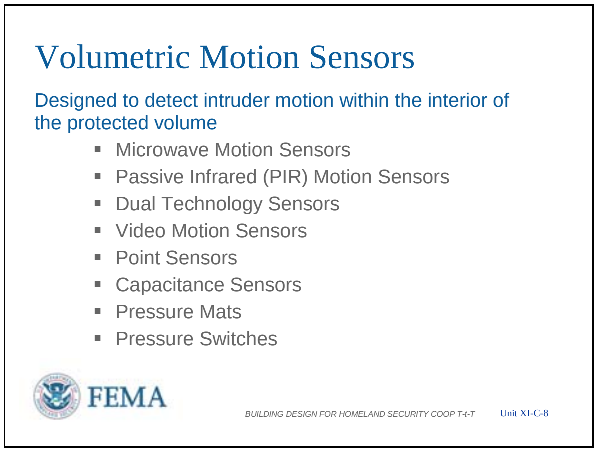
Balanced magnetic switches (BMSs) are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry.

Passive ultrasonic sensors detect acoustical energy in the ultrasonic frequency range, typically between 20 and 30 kilohertz (kHz). They are used to detect an attempted penetration through rigid barriers (such as metal or masonry walls, ceilings, and floors), and windows and vents covered by metal grilles, shutters, or bars if these openings are properly sealed against outside sounds.

Grid wire sensors consist of a continuous electrical wire arranged in a grid pattern. The wire maintains an electrical current. An alarm is generated when the wire is broken. The sensor detects forced entry through walls, floors, ceilings, doors, windows, and other barriers. (This type sensor can be used well with structural vibration sensors).

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-C-8



Volumetric Motion Sensors

Designed to detect intruder motion within the interior of the protected volume:

- Microwave Motion Sensors
- Passive Infrared (PIR) Motion Sensors
- Dual Technology Sensors
- Video Motion Sensors
- Point Sensors
- Capacitance Sensors
- Pressure Mats
- Pressure Switches

Microwave motion sensors use high-frequency electromagnetic energy to detect an intruder's motion within the protected area. Interior or sophisticated microwave motion sensors are normally used.

Interior microwave motion sensors are typically monostatic; the transmitter and the receiver are housed in the same enclosure (transceiver).

Sophisticated microwave motion sensors may be equipped with electronic range gating. This feature allows the sensor to ignore the signals reflected beyond the settable detection range. Range gating may be used to effectively minimize unwanted alarms from activity outside the protected area.

Passive infrared (PIR) motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.

Dual technology sensors combine two different technologies in one unit to minimize the generation of alarms caused by sources

INSTRUCTOR NOTES	CONTENT/ACTIVITY

other than intruders.

- Stereo Doppler is a dual channel microwave design. The combination of a Microwave (MW) Sensor and a Passive Infrared Sensor (PIR) must activate simultaneously to create an alarm.

Video motion sensors generate an alarm when an intruder enters a selected portion of a CCTV camera's field of view. The sensor processes and compares successive images between the images against predefined alarm criteria. There are two categories of video motion detectors, analog and digital. Analog detectors generate an alarm in response to changes in a picture's contrast. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image.

Point sensors are used to protect specific objects within a facility. These sensors (sometimes referred to as proximity sensors) detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches.

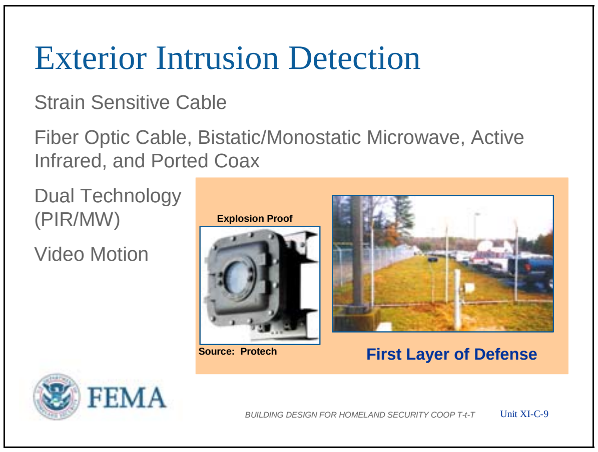
Capacitance sensors detect an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground. Think of some types of car alarms.

Pressure mats generate an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Pressure switches are mechanically activated contact switches or single ribbon switches.

VISUAL XI-C-9



Exterior Intrusion Detection Sensors

- Strain Sensitive Cable - fences and gates
- Fiber Optic Cable - fences, gates, and gravel pathways
- Bistatic/Monostatic Microwave - line of sight, clear zones
- Active Infrared - portals, short perimeter gap filters
- Ported Coax - exterior clear zones
- Dual Technology (PIR/MW) - portals and gap fillers
- Video Motion - volumetric traffic, open areas

Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones between fences or around buildings, for protecting materials and equipment stored outdoors within a protected boundary, or in estimating the POD (Probability of Detection) for buildings and other facilities.

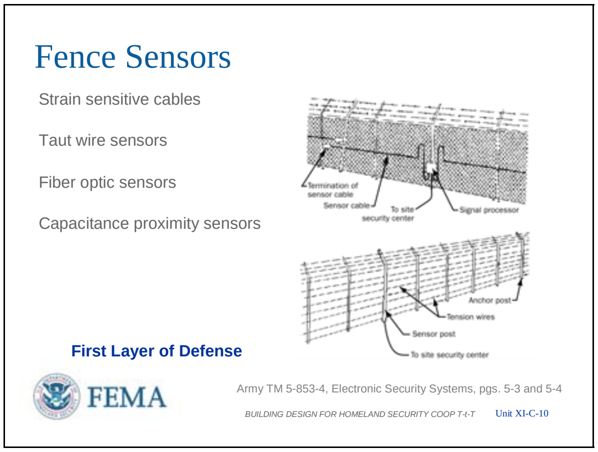
Because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms than interior sensors. Inclement weather conditions (e.g., heavy rain, hail, and high wind), vegetation, the natural variation of the temperature of objects in the detection zone, blowing debris, and animals are major sources of unwanted alarms.

The combination of MW (**M**icro**w**ave) and PIR (**P**assive **I**nfra**r**ed) works well to eliminate weather, birds/animals, vegetation, blowing debris, hail etc from causing false

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

alarms.

VISUAL XI-C-10



Fence Sensors

- Strain sensitive cables
- Taut wire sensors
- Fiber optic sensors
- Capacitance proximity sensors

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts (e.g., climbing, cutting, or lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain.

Strain sensitive cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical distortions or stress resulting from fence motion.

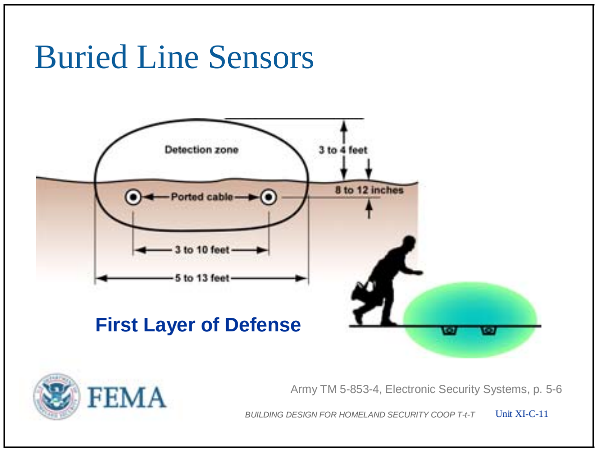
Taut wire sensors combine a physically taut-wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end.

Fiber optic sensors are functionally equivalent to the strain-sensitive cable sensors previously discussed. However, rather than electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed to determine whether an alarm should be initiated.

Capacitance proximity sensors measure the electrical capacitance between the ground and an array of sense wires. Any variations in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-C-11



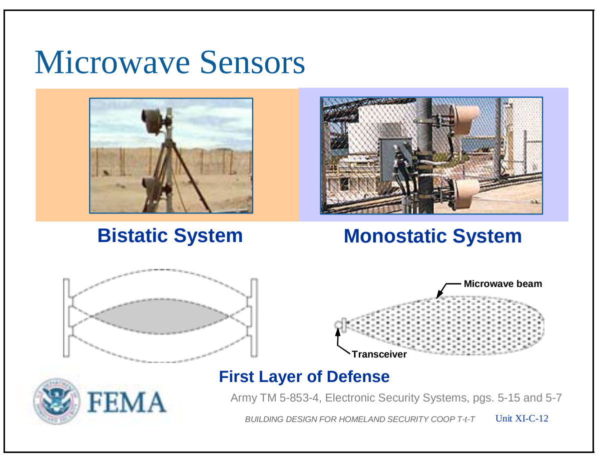
Buried Line Sensors

A buried line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field.

Buried line sensors have several significant features:

- They are hidden, making them difficult to detect and circumvent.
- They follow the terrain's natural contour.
- They do not physically interfere with human activity, such as grass mowing or snow removal.
- They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles.

VISUAL XI-C-12



Microwave (MW) Sensors

- Bistatic system
- Monostatic

Microwave intrusion detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use the same antenna.

A bistatic system uses a transmitter and a receiver that are typically separated by 100 to 1,200 feet and that are within direct line of sight of each other.

Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

for the transmitter and receiver, which are usually combined into a single package.

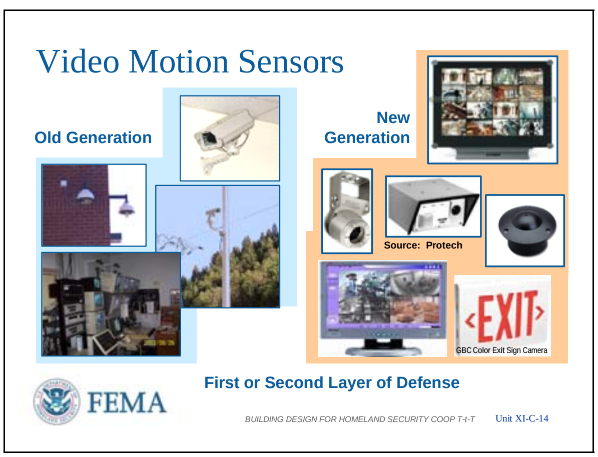
VISUAL XI-C-13

Infrared (IR) Sensors

The IR sensors are available in both active and passive models. An active sensor generates one or more near-IR beams that generate an alarm when interrupted. A passive sensor detects changes in thermal IR radiation from objects located within its field of view.

Active sensors consist of transmitter/receiver pairs. The transmitter contains an IR light source (such as a gallium arsenide light-emitting diode [LED]) that generates an IR beam. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

VISUAL XI-C-14



This slide shows old generation and new generation video motion sensors.

Video Motion Sensors

Video motion sensors are available on most digital video recorders used in security applications.

- They can be programmed to activate alarms, initiate recording, or any other designated action when motion is detected by a security camera.
- Some digital video recorders can be programmed to monitor very specific fields of view for specific rates of motion in order to increase effectiveness and minimize extraneous detections.
- Video motion sensors can also greatly improve the efficiency of security personnel monitoring security cameras by alerting them when motion is detected.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-C-15

Inspection Devices are primarily used in manual systems as they are operated by the guards as part of the entry process. These devices include

- Magnetic Wand / Magnetometer to detect weapons
- X-Ray to inspect packages
- Sniffers / Swabs to detect chemicals / explosives

Entry Control Systems and Technology

- Coded Devices
- Credential Devices
- Biometric Devices
- Inspection Devices

The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals. These means of entry control can be applied manually by guards or automatically by using entry control devices.

- In a <u>manual system</u>, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry.
- In an <u>automated system</u>, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage.

All entry control systems control passage by using one or more of three basic techniques (e.g., something a person knows, something a person has, or something a person is or does). <u>Automated entry control</u> devices based on these techniques are grouped into <u>three categories</u>: coded, credential, and biometric devices.

Inspection Device information is found under Visual in the left column.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-C-16

Coded Devices

- Electronic Keypad Devices
- Computer Controlled Keypad Devices

Coded devices operate on the principle that a person has been issued a code to enter into an entry control device. This code will match the code stored in the device and permit entry. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Electronically coded devices include electronic and computer controlled keypads.

Electronic keypad devices are similar to telephone keypads (12 keys). This type of keypad consists of simple push-button switches that, when depressed, are decoded by digital logic circuits. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds.

Computer controlled keypad devices are devices similar to electronic keypad devices, except they are equipped with a microprocessor in the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the keys are depressed and may provide additional functions, such as personal ID and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

PRECAUTIONS:

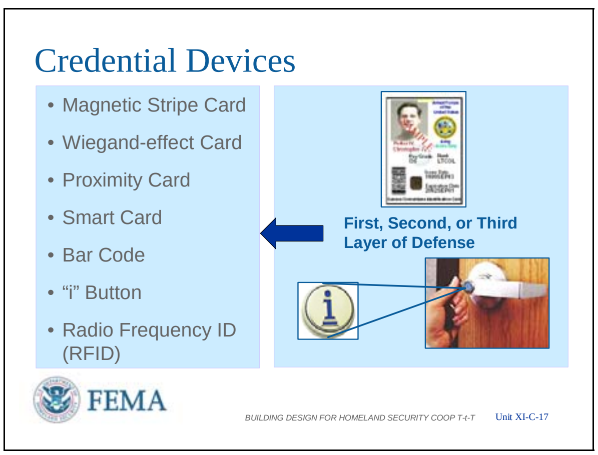
- Care should be taken so other persons cannot observe individuals entering

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

their assigned code. Installation of an opaque shield around the device aids in control of unauthorized observations. This helps to eliminate the use of another's code to gain entry into an unauthorized area.

- Also, care should be taken to replace coded pads that show wear from repeated code entries. Code compromise may be accomplished by attempting use of the worn keys (which results in less permutations of the combination to gain access).
- Individual codes are best for access control and accountability.

VISUAL XI-C-17



Credential Devices

- Magnetic Stripe Card
- Wiegand-effect Card
- Proximity Card
- Smart Card
- Bar Code
- Button
- Radio Frequency Identification Device

A credential device identifies a person having legitimate authority to enter a controlled area. A coded credential (e.g., plastic card or key) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read.

A **magnetic stripe card** is a strip of magnetic material located along one edge of the card that is encoded with data (sometimes encrypted). The data are read by moving the card past a magnetic read head.

A **Wiegand-effect card** contains a series of small-diameter, parallel wires approximately

½-inch long, embedded in the bottom half of the card. The wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power.

A **proximity card** is not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. Several techniques are used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an integrated circuit embedded in the card to generate a code that can be magnetically or electrostatically coupled to the reader.

A **smart card** is embedded with a microprocessor, memory, communication circuitry, and a battery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry control information and other data may be stored in the microprocessor's memory.

A **bar code** consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry control applications because it can be easily duplicated.

The **"i" button** is a computer chip enclosed inside a 16mm stainless steel can. The “i” button can grant its owner access to a building, a PC, a piece of equipment, or a vehicle. Some “i” buttons can be used to store cash for small transactions, such as transit systems, parking meters, and vending machines. Also used as an electronic asset tag to store information needed to keep track of valuable capital equipment.

The Radio Frequency Identification Device (RFID) Systems rely on a radio frequency identification chip implanted in an access card, i.e., Proximity, Smart, or similar which transmits card owner information wirelessly.

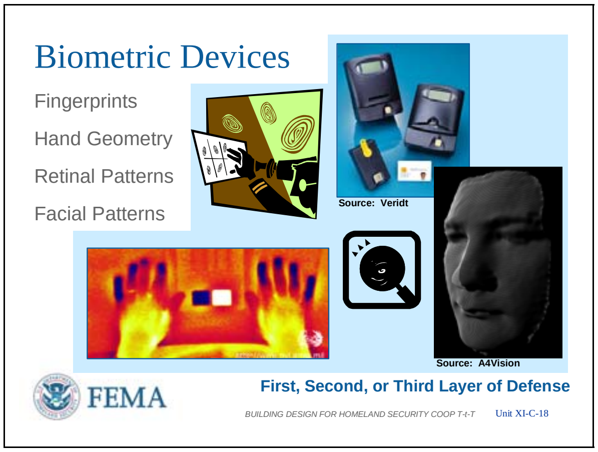
Although this is leading edge technology, significant security and privacy issues exist to a level that government agencies eager to use this technology have abandoned their acceptance and use until the security and privacy issues are resolved. The ability for the remote operation of this technology gives it great interest for now and the future.

Without a biometric device necessary to be used with a credential device the only thing to be verified from an after incident entry point log review is “the device” was used to enter the area. Without some other means of identification (biometrics or Personal Identification Number), a person other than the owner can use a lost or stolen card, and cannot be tied to the card.

In the absence of biometric devices, anti-pass back devices, and procedures should be in place to eliminate unauthorized usage. Assign responsibility of the person issued the device for ensuring two people cannot use the same credential device. This is commonly occurs when one tells another they “forgot” their device.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-C-18



Biometric Devices

- Fingerprints
- Hand Geometry
- Retinal Patterns
- Facial Recognition

The third basic technique used to control entry is based on the measurement of one or more physical or personal characteristics of an individual. Because most entry control devices based on this technique rely on measurements of biological characteristics, they have become commonly known as biometric devices. Characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood-vessel patterns have been used for controlling entry. Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template. If a match is found, entry is granted.

Fingerprint verification devices use one of two approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.

Hand geometry devices use a variety of physical measurements of the hand, such as finger length, finger curvature, hand width, webbing between fingers, and light transmissivity through the skin to verify

INSTRUCTOR NOTES	CONTENT/ACTIVITY

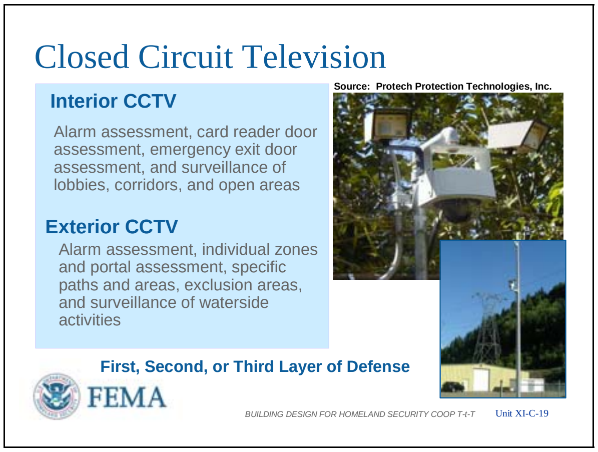
identity. Both two- and three-dimensional units are available.

Retinal pattern is based on the premise that the pattern of blood vessels on the human eye's retina is unique to an individual. While the eye is focused on a visual target, a low-intensity IR light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood-vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature.

Facial Recognition is a facial identification/verification reader system with touch screen PIN (Personal Identification Number) and 3D facial biometric access. An audio request for a PIN entry references the 3D face template stored in the database with the corresponding PIN. Verification is made from the correct PIN entry matching the reader image. Night, changing light conditions, and motion will not change the high rate of accuracy according to the manufacturer.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-C-19



Closed Circuit Television Systems

- Interior CCTV - alarm assessment, card reader door assessment, emergency exit door assessment, and surveillance of lobbies, corridors, and open areas
- Exterior CCTV - alarm assessment, individual zones and portal assessment, specific paths and areas, exclusion areas, and surveillance of waterside activities
- Transmission media includes twisted pair telephone cable, coaxial TV cable, LAN (Local Area Network) cable, fiber optics, and wireless. Each has cost, line length, resolution, reliability, and quality considerations. Security, encryption, and redundancy are also concerns throughout the length of run from sensor to monitor/alarm.
- Only color should be installed. There is very little use of black and white television when attempting to assemble a description of an individual who is wearing clothing in the shades of gray to white. Were they wearing blue jeans, or black or green trousers?

VISUAL XI-C-20

Security Operations Center

The operator monitoring the alarms and displays of a Security Operations Center is probably the most ineffective sensor in the system.

- The workspace should be conducive to maintaining attention, not like the two smaller photos where the monitors are outside the normal line of sight and in glare.
- The workspace should have some hardening as it is a single point of vulnerability in the system where response is initiated.
- Visual and/or audio alerts need to draw the

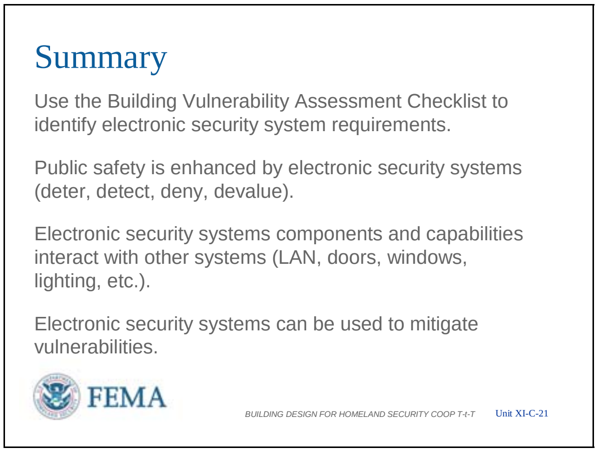
INSTRUCTOR NOTES	CONTENT/ACTIVITY

operators attention to alarms and focus the operator on the specific monitor with the detection information requiring real-time assessment for action.

- CCTV can assist in these alerts using image-based motion detection or SMART CCTV where attention is drawn to the camera that pan/tilts/zooms to the location from which the alarm is coming, such as the door where a balanced magnetic switch loses continuity or a motion detector senses motion where none is expected.
- Forwarding of alarms to cell phones, pagers, personal digital assistants, or radios keeps the staff on notice that a problem exists. It also allows the operator to take a bathroom break without having to have another person stand-in at the monitors.
- Digital Video Recorders (DVR) store more information with better quality resolution for not only detection, but also assessment and future potential criminal proceedings.
- Like fire alarm systems, all physical lines carrying alarm information should be supervised to identify any tampering with a line and to ensure functionality. Backup feeds or alternate feeds following different routes also increase reliability, especially in computer-based IP (Internet Protocol) systems.
- Since electric power is needed for system operation throughout the system, backup power with redundant lines should also be considered.

INSTRUCTOR NOTES

VISUAL XI-C-21



CONTENT/ACTIVITY

Summary

Remember all the different components of the system must support each others' function. For example, the best barriers are those tied to a detection system, like a strain sensitive cable alarm sensor on a chain link fence, with a steel cable woven into the fence, delay function, and overseen by an assessment method, such as a CCTV system.

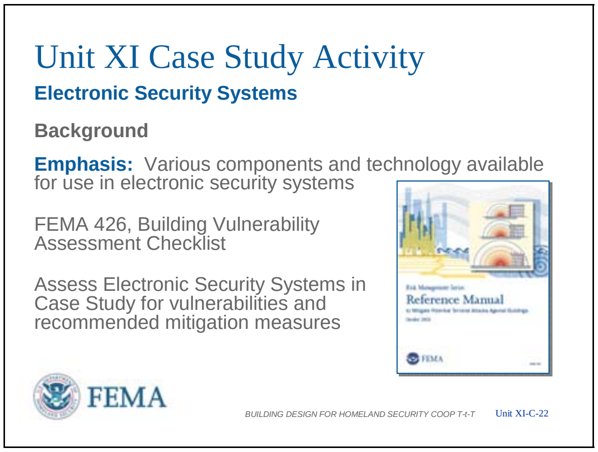
The best practice is to evaluate products against operational and desired results criteria. This has proven to be a problem during attempted evaluations conducted by agencies trying to compare two different systems. System operating protocols were different from each other and, as a result, could not produce compatible/comparable results.

NOTE: All system control boxes should be equipped with an intrusion detection alarm which annunciates at the box and at the system control console, and is tied electronically to the events report log to be acknowledged, investigated (response) and cleared on the log. A link to CCTV recorded events is also advisable for immediate visual response/review.

- Use the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** to identify electronic security system requirements.
- Public safety is enhanced by electronic security systems (deter, detect, deny, devalue).
- Electronic security systems components and capabilities interact with other systems (LAN, doors, windows, lighting, etc.).
- Electronic security systems can be used to mitigate vulnerabilities.

INSTRUCTOR NOTES

VISUAL XI-C-22



Refer participants to **FEMA 426**, Vulnerability Checklist Section 12 and Tab XI-A or XI-B in the Student Manual for the selected Case Study activity.

At the end of 10 minutes, reconvene the class and facilitate group reporting. The plenary session should take 5 minutes.

CONTENT/ACTIVITY

Student Activity

In this unit, the emphasis was upon the various components and technology available for use in electronic security systems.

The **Building Vulnerability Assessment Checklist in FEMA 426 (Table 1-22, pages 1-81 to 1-89)** can be used as a screening tool for preliminary building design vulnerability assessment and assessment of existing buildings.

Activity Requirements

- Working in small groups, refer to the selected Case Study to determine answers to the worksheet questions.
- Then review results to identify vulnerabilities and possible mitigation measures.

Take 10 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

In the next unit, you will finalize and present the Case Study Results determined by your team. This will include preparation and presentation of the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk, although other vulnerabilities and recommended mitigation measures may also be presented. Prioritize the top three risks and the top three recommended mitigation measures with rationale and justification. Include any consideration for changes to security systems per this instruction unit.

UNIT XI (C) CASE STUDY ACTIVITY: ELECTRONIC SECURITY SYSTEMS (COOP Version)

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

Requirements

Refer to the Appendix C Case Study to determine answers to the questions. Then review results as a team to identify vulnerabilities and possible mitigation measures.

Activity # 1: Complete the selected vulnerability checklist questions in the following Vulnerability Questions table.

Activity # 2: Upon completion of the questions refer back to the vulnerability ratings determined in the Unit IV (C) Student Activity. Based on this more detailed analysis, decide if any vulnerability rating needs adjustment. Adjust the Risk Matrix poster accordingly for any changes in vulnerability rating.

Activity # 3: Select mitigation measures to reduce vulnerability and associated risk from the site, layout, and building perspectives. Concentrate on the three highest risk ratings on the Risk Matrix poster as adjusted by Activity # 2. Use the Electronic Security System Mitigation Measures table found at the end of this unit to capture this information.

Activity # 4: Consider the mitigation measures of Activity #3 to be installed, estimate the new vulnerability ratings as if these measures were in place, and calculate the new risk ratings. Capture your information in the Electronic Security System Mitigation Measures table.

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
	Perimeter Systems		
12.1	Are black/white or color CCTV (closed circuit television) cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom?	Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management	***The parking lot behind the CI/BC office is well lit and monitored by older generation analog CCTV cameras using telephone wires that are connected to video displays in the CI/BC Security Officer's office and recorded on standard VHS tape.***

	Are they analog or digital by design? What is the number of fixed, wireless and pan-tilt-zoom cameras used? Who are the manufacturers of the CCTV cameras? What is the age of the CCTV cameras in use?	must be able to meet daily security challenges from a cost-effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design. Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. Reference: *GSA PBS P-100*	***The CCTVs are commercial grade black and white with a 180-degree field of view that the security officer can control via the display panel.*** ***The front parking lot is lit, but not monitored.***
12.2	Are the cameras programmed to respond automatically to perimeter building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***No cameras respond automatically to alarms or have video motion capability.*** ***Video controls are manual and available to the CI/BC Security Officer via the display panel.***
12.4	Are panic/duress alarm buttons or sensors used, where are they located, and are they hardwired or portable?	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other high risk locations by assessment. Reference: *GSA PBS P-100*	***There are no panic/duress alarms or sensors used.***
12.5	Are intercom call boxes used in parking areas or along the building perimeter?	See Item 12.4.	***There are no intercom call boxes used on the site.***

12.7	Who monitors the CCTV system?	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	***The CI/BC security officer.***
12.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	***The CCTV system is connected to the Computer Center Bus. This bus is supplied by the Uninterruptible Power Supply for the building and the backup diesel electric generator.***

Electronic Security System Mitigation Measures
(COOP Version)

This table is filled out because there is less possibility of great variation among assessment teams in this subject area.

Asset-Threat / Hazard Pair	Current Risk Rating	Suggested Mitigation Measure	Revised Risk Rating
1. ***All Assets / Vehicle Bomb***	***High***	***Upgrade Closed Circuit Television (CCTV)s to digital and use Digital Video Recorders (DVR).*** ***Install exterior CCTVs to monitor front parking and expand back parking coverage, including loading dock.*** ***Install interior CCTVs to monitor interior lobbies, utility rooms, and access to secure spaces.*** ***Link cameras to alarms and install video motion where appropriate.*** ***Goal: Deter and Detect***	***Medium***

Asset-Threat / Hazard Pair	Current Risk Rating	Suggested Mitigation Measure	Revised Risk Rating
2. ***Functions* *(Engineering / IT Technicians, Data Center Communications, and Security)* *and* *Critical Infrastructure (Mechanical Systems and IT / Communications) / Chemical (CBR Attack)***	***High***	***Evaluate installation of basic chemical sensors on outside air intake of HVAC system or acquisition of portable sensors for use by Building Security.*** ***Ensure coverage of intakes and mechanical systems equipment using CCTV and alarms to prevent tampering.*** ***Consider automatic shutdown of all air handling equipment upon activation of sensors and alarms.*** ***Goal: Detect***	***High to Medium***
3. ***Functions* *(Engineering / IT Technicians, Data Center Communications, and Security)* *and* *Critical Infrastructure (Mechanical Systems and IT / Communications) / Biological (CBR Attack)***	***High***	***Evaluate acquisition of portable or basic level biological sensors for use by Building Security.*** ***Ensure coverage of intakes and mechanical systems equipment using CCTV and alarms to prevent tampering.*** ***Consider automatic shutdown of all air handling equipment upon activation of sensors and alarms.*** ***Goal: Detect***	***High to Medium***

Asset-Threat / Hazard Pair	Current Risk Rating	Suggested Mitigation Measure	Revised Risk Rating
4. ***Functions*** ***(Engineering / IT Technicians, Data Center Communications, and Security) and*** ***Critical Infrastructure*** ***(Mechanical Systems and IT / Communications) /*** ***Radiological (CBR Attack)***	***High***	***Evaluate acquisition of portable or basic level radiological sensors for use by Building Security.*** ***Ensure coverage of intakes and mechanical systems equipment using CCTV and alarms to prevent tampering.*** ***Consider automatic shutdown of all air handling equipment upon activation of sensors and alarms.*** ***Goal: Detect***	***Medium***

This page intentionally left blank

Unit XII (C)

COURSE TITLE

Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer

TIME 135 minutes

UNIT TITLE

Case Study

OBJECTIVES

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

SCOPE

The following topics will be covered in this unit:

1. Activity: Preparation and presentation of the highest risks identified by the assessment groups, the vulnerabilities identified for these risks, and recommended mitigation measures to reduce vulnerability and risk.
   a. Prioritize the top three risks as well as the top three recommended mitigation measures with rationale and justification. This includes any consideration for changes to the Risk Matrix from knowledge gained in Units IX, X, and XI.
   b. Identify all requirement gaps that need to be provided for Cooperville Information / Business Center to be a fully functional COOP facility supporting the U.S. Department of Artificial Intelligence.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings:*
   a. Pages 2-50 to 2-58
   b. Pages 3-50 to 3-52
   c. Chapter 5
   d. Appendix D
2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 5-1 to 5-18
3. Case Study – Appendix C: COOP, Cooperville Information / Business Center

4. Student Manual, Unit XII (C) (info only – do not list in SM)
5. Unit XII (C) visuals (info only – do not list 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 XII (C)
4. Student Manual, COOP Case Study (C) (one per student)
5. Overhead projector or computer display unit
6. Unit XII (C) visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart, paper, easel, and markers (one per team)

UNIT XII (C) OUTLINE

	Time	Page
XII. Case Study	135 minutes	IG XII-C-1
1. Introduction and Unit Overview	20 minutes	IG XII-C-5
2. Activity: 45 minute Preparation and 60 minute Presentation by Groups	105 minutes	IG XII-C-20
3. Review of School Solutions (Mitigations Measures, Blast, CBR, and Cost)	10 minutes but variable based on time available	IG XII-C-21
4. Activity: Case Study – Student Presentation of Results		IG XII-C-39

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** There is no specific content that can be linked to the local area. All actions of this instruction focus on the Case Study, Appendix C, Cooperville Information / Business Center.

  The Instructor will review the Case Study, Appendix C, Cooperville Information / Business Center, DoD Antiterrorism Standards, DHS Interagency Security Criteria, and understand the parameters for the Design Basis Threat and Levels of Protection and their impact upon the assessment. Additionally, review of the school solution mitigation measures, blast analysis, CBR analysis, and costs will ensure a smooth presentation in a time-constrained environment.

The first part of this instruction unit is not so much to repeat the Case Study contents of Unit 1, but to provide an opportunity for review and allow questions before students prepare their presentations within their assessment groups.

- **Optional Activity:** There are no optional activities in this unit.
- **Activity:** The students will prepare and present the top three risks identified by the assessment group, the vulnerabilities identified for these risks, and the top three recommended mitigation measures to reduce vulnerability and risk. The group will prioritize the top three risks as well as the top three recommended mitigation measures with rationale and justification. Includes any consideration for changes from the knowledge obtained in Units IX, X, and XI. The students will also present any COOP requirements gaps identified in the CI/BC building that are needed to support US Department of Artificial Intelligence Requirements.
- Refer students to their Student Manuals for worksheets and activities.
- Direct students to the appropriate page (Unit #) in the Student Manual.
- Instruct the students to read the activity instructions found in the Student Manual.
- 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. Ask for volunteer groups to determine the order of presentation. Capture the answers provided by the students for future update of the course.
- After the students have completed their presentations, **as time permits**, present the "school solution" mitigation measures, blast analysis, CBR analysis, and associated costs and decision process. Be prepared to answer any student questions.
- Ask for and answer questions.

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

(1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>

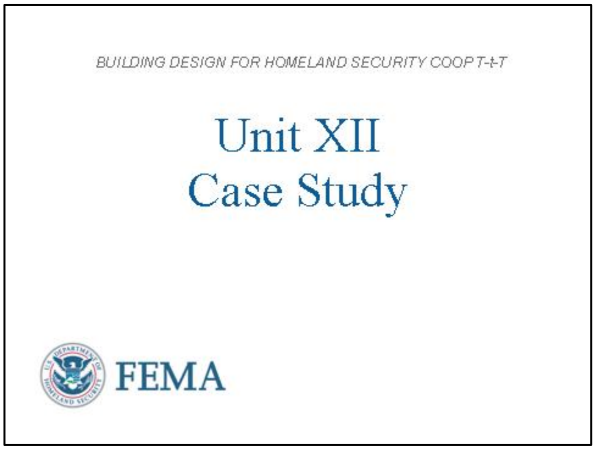
(2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>

(3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-1



Introduction and Unit Overview

This is the Unit XII Case Study activity. This unit will review the Cooperville Information / Business Center site and building portfolio, DoD Antiterrorism Standards, DHS Interagency Security Criteria, and the parameters for the Design Basis Threat and Levels of Protection.

Students will prepare and present the top three risks identified by the assessment group, the vulnerabilities identified for these risks, and the top three recommended mitigation measures to reduce vulnerability and risk. The groups will prioritize the top three risks as well as the top three recommended mitigation measures with rationale and justification. Consider any changes to the Risk Matrix due to knowledge gained in Units IX, X, and XI..

VISUAL XII-C-2

Unit Objectives

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

1. Explain building security design issues to a building owner for consideration prior to a renovation or new construction.

2. Explain the identification process to arrive at the high risk asset-threat/hazard pairs of interest.

3. Justify the recommended mitigation measures, explaining the benefits in reducing the risk for the high risk situations of interest.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-3

Cooperville Information / Business Center

The Case Study will be a comprehensive review and practical application of **FEMA 426 / FEMA 452**.

In this unit, the following topics will be presented:

- Company Functions
- Company Infrastructure
- Threats/Hazards (including Design Basis Threat and Levels of Protection)
- Vulnerabilities (including Impact and Mitigation)

VISUAL XII-C-4

Cooperville Information / Business Center

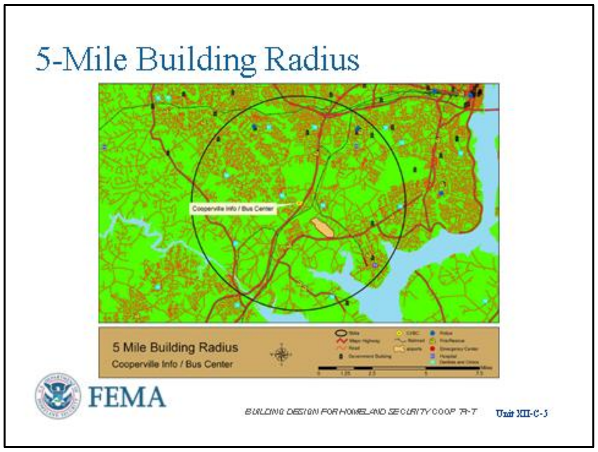
The Cooperville Information / Business Center supports approximately 1,000 users and 100 applications as a primary data center and as a disaster recovery backup site. It also provides temporary office space as required by regular and traveling clients.

CI/BC has over 75 employees and approximately 40 employees are in the building during shift change.

- Regional computer center
- Suburban business park
- Customers and neighbors

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

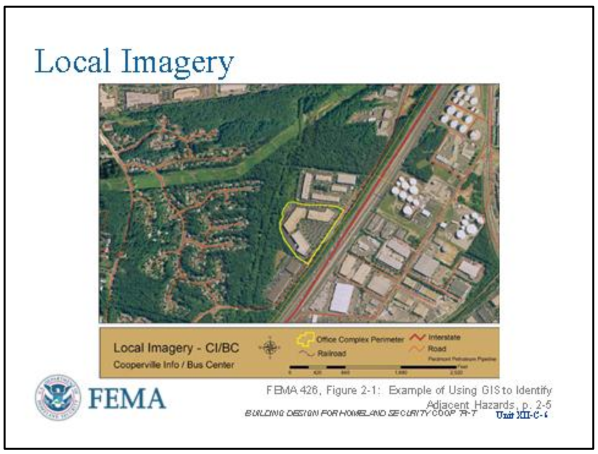
VISUAL XII-C-5



5-Mile Building Radius

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

VISUAL XII-C-6



Local Imagery

The office building is part of a corporate business park. CI/BC does not control the front parking area, signage, or other general site conditions such as stormwater drainage, lighting, or vehicle and pedestrian traffic flow and movement. The business park is responsible for grounds maintenance to include cutting the grass, planting flowers, trimming trees, sweeping the parking lot, and towing unauthorized vehicles. Trash service is the responsibility of tenants. CI/BC has a large dumpster located at the rear of the loading dock area approximately 50 feet from the building.

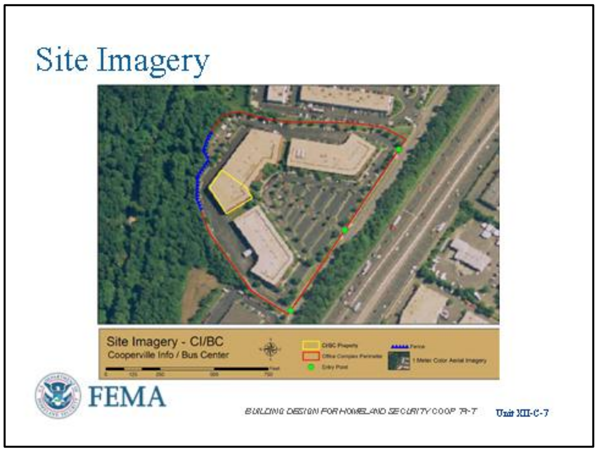
CI/BC receives the mail and packages at the front office lobby desk. Large packages and equipment are delivered to the rear loading dock. CI/BC does not have a separate mail room, but does have an internal administrative space with copiers, printers, supplies, and staff mailboxes. The front desk receptionist is responsible for sorting and screening all mail.

The business park is adjacent to a major interstate highway and there are a number

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

of storage tanks, manufacturing and production facilities, and other commercial properties across the interstate.

VISUAL XII-C-7

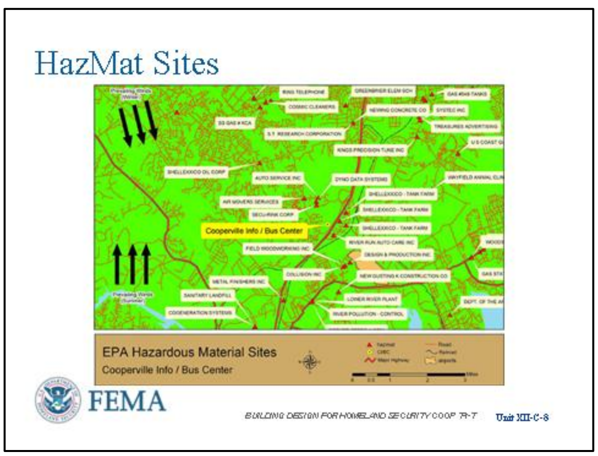


Office Building (Site Imagery)

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

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

VISUAL XII-C-8

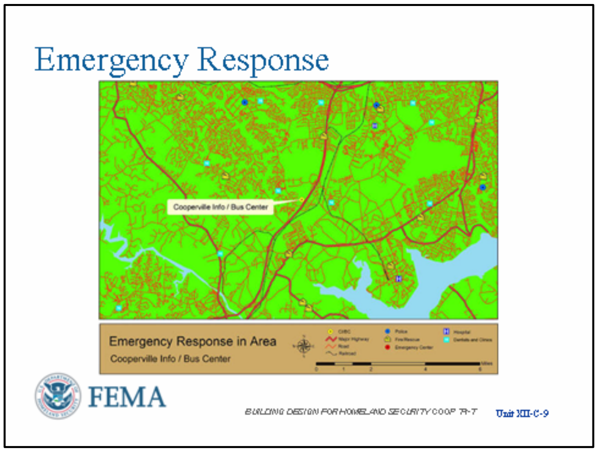


HazMat Sites

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

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

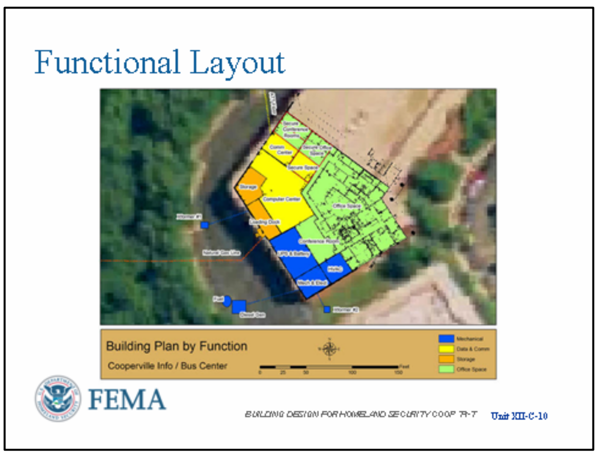
VISUAL XII-C-9



Emergency Response

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

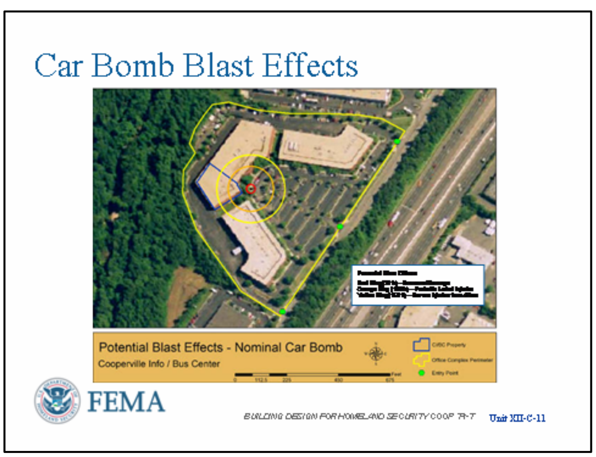
VISUAL XII-C-10



Functional Layout

- Downstairs: Computer Center, Communications, Storage, Secure Space, Conference Rooms (Secure and Unclassified) and Business Center (Office Space)
- Downstairs: Highbay, loading dock, mechanical and electrical (M&E) room, HVAC room
- Upstairs: Executive Offices and Staff

VISUAL XII-C-11



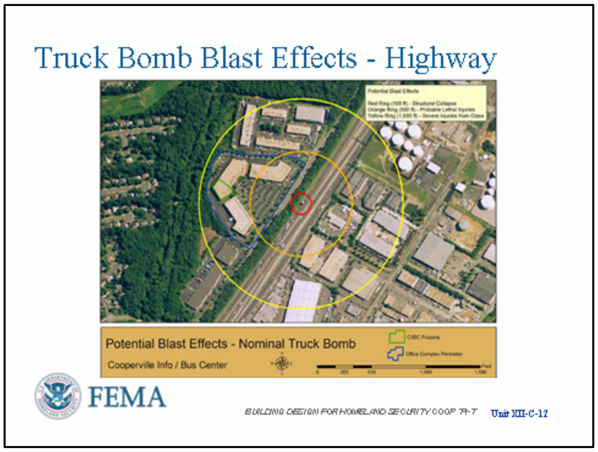
Car Bomb Blast Effects

The nominal range-to-effects chart radius of influence of a small car bomb detonation at the front entrance indicates that the building would experience significant damage, but would likely not suffer progressive collapse. The front façade of the building is over 50 percent glass and has an 8-foot overhang. The terrain slopes upward from the parking lot to the main entrance, and landscaped with flowerbeds and trees. Key staff and Business Center clients would probably receive severe

INSTRUCTOR NOTES	CONTENT/ACTIVITY

injuries and administrative functions destroyed, but the Computer Center and Communications functions would likely survive relatively intact.

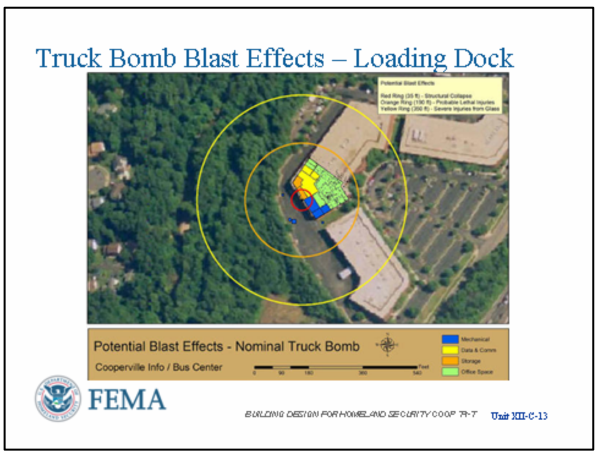
VISUAL XII-C-12



Truck Bomb Blast Effects - Highway

A truck bomb detonation occurring on the interstate would also significantly damage the CI/BC building, primarily glass breakage and potentially some structural damage. If the truck bomb were to detonate near the tank farm, the ensuing plume would impact the CI/BC building.

VISUAL XII-C-13

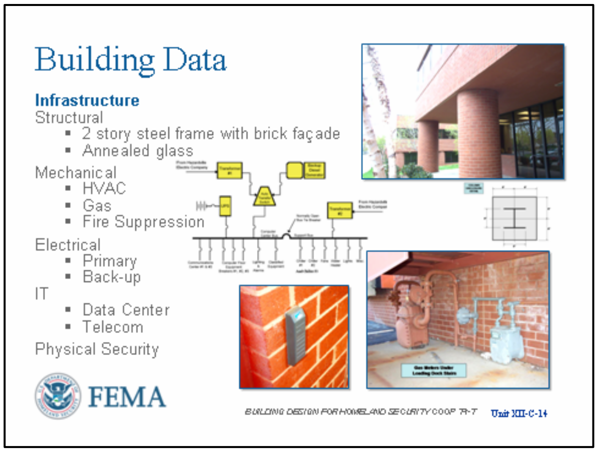


Truck Bomb Blast Effects – Loading Dock

A truck bomb detonation at the rear of the CI/BC building at the loading dock would result in significant structural damage and potential localized collapse. The blast would greatly affect the Computer Center, Communications, and other critical functions. Critical infrastructure would also be seriously affected, including the mechanical/electrical room.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

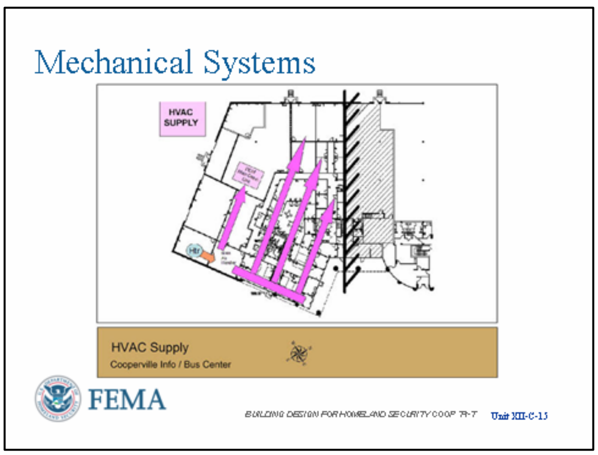
VISUAL XII-C-14



Building Data (Infrastructure)

- Structural -- two-story steel frame structure with a brick facade and annealed glass.
- Mechanical – HVAC cooling towers, natural gas, and water sprinkler system
- Electrical – backup generator
- IT – computer center and communications
- Physical Security – access control

VISUAL XII-C-15

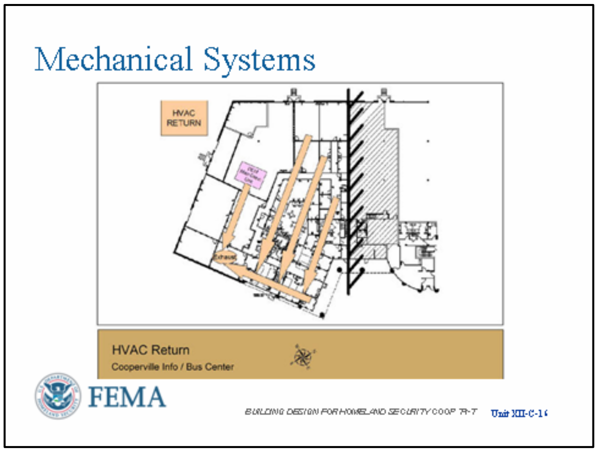


Mechanical Systems – HVAC Supply

The air used to heat or cool the CI/BC building is filtered in the HVAC room using standard industrial grade MERV 8 filters. Outside make-up air is brought in through a vent in the wall located at ground level.

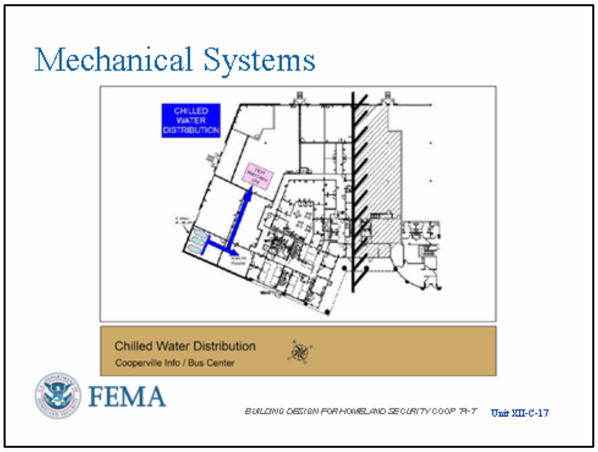
The Computer Data Center has two additional air cooling units located in the Data Center and uses the main chilled water supply. The Data Center maintains a slight net positive pressure compared to the rest of the building.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**
VISUAL XII-C-16	**Mechanical Systems – HVAC Return**



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

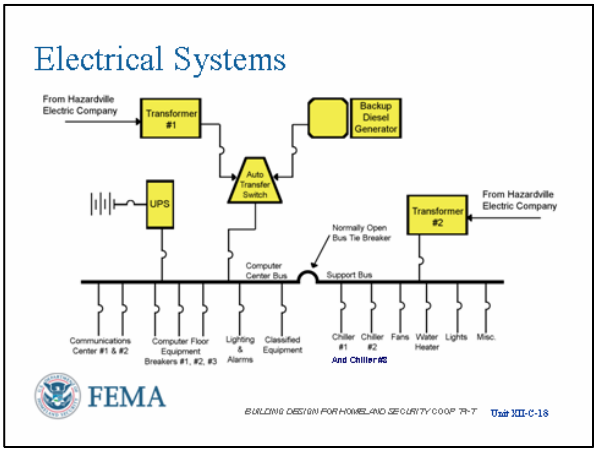
VISUAL XII-C-17	**Mechanical Systems – Chilled Water**



Chiller operation along with chilled water and condenser water flow are managed from a single control unit in the M&E room. A single chilled water pump provides adequate flow for all cooling situations; a backup pump is available at the push of a button. The same is true for the condenser water pumps. There is one supply and return line between the chiller and the Data Center.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

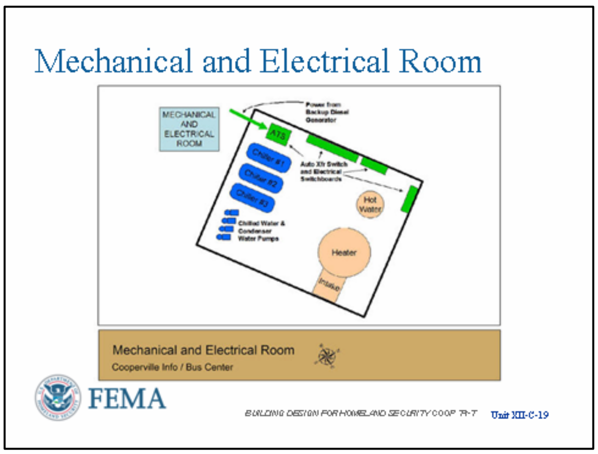
VISUAL XII-C-18



Electrical System

CI-BC's electrical loads are divided between two main electrical buses, the Computer Center Bus (CCB) and the Support Bus (SB). They are located in separate "closets" of the building. A tie breaker allows the buses to be connected, so they can be powered by a single main transformer, or to allow SB loads to be carried by the backup diesel generator. A digital energy management system monitors the electrical system and provides indications, alarms, and instructions.

VISUAL XII-C-19



Mechanical and Electrical Room

Typical of many commercial office buildings, the mechanical and electrical systems share common utility penetetrations and floor space. There are no redundant utility feeds to the building from different directions, but utilities loop around the buildings in the office park, although they connect to the same radial feeder outside the office park.

VISUAL XII-C-20

IT (Information Technology)

The Computer Center is the heart of the Cooperville Information / Business Center (CI/BC) operation.

The Computer Center is composed of several interconnected systems and one independent system for classified data processing. The systems run either VMS, Unix, or Windows.

Data:
CI/BC has two T1 lines and one T3 line connected at the demark to ATT's high

INSTRUCTOR NOTES	CONTENT/ACTIVITY

performance backbone network. The ATT fiber connectivity provides more than enough bandwidth for CI/BC's current needs and planned future expansion.

Telecom and Network Connections:

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

Voice

NEC DS2000 telephone systems that come with an 8-slot cabinet that can handle 32 lines from 48 stations.

VISUAL XII-C-21

Physical Security

CI/BC uses a layered approach to physical security:

The outermost physical security layer is provided by a contract security firm and the Defense Protective Service (DPS).

- The parking lot behind the CI/BC office is well lit and monitored by older generation analog CCTV cameras.
- The front parking lot is lit, but not monitored.

CI/BC's middle layer of security is the building envelope.

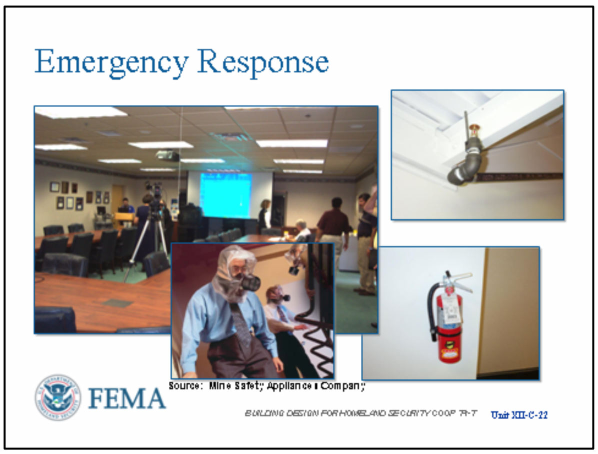
- The building is monitored by door and window alarms, which connect to ADT, the nationwide alarm company.

The innermost layer of physical security involves the Computer Center, Communications Center, and Secure Spaces (offices and conference rooms).

INSTRUCTOR NOTES	CONTENT/ACTIVITY

- Equipped with locked doors, rooms meet the government's requirements for handling classified material.
- Only authorized employees possess the necessary proximity cards and PINs to gain access.
- The receptionist handles badging of visitors and Business Center clients and works with security to provide appropriate access.
- Access to Computer Center and Communications is through the secure area of the Information Division on the mezzanine.

VISUAL XII-C-22



Emergency Response

In the event of an emergency, CI/BC senior management uses the large conference room as an emergency operations center and shelter-in-place area. The room is equipped with network and telephone connections and cell phones are able to receive a signal.

The nearest fire station is approximately 2½ miles north of the CI/BC building. Seven others are within 5 miles of the site. Firefighters are trained as Emergency Medical Technicians (EMTs) and Hazardous Material Technicians. Many are also skilled in technical rescue (high places, confined spaces, etc.). These stations also dispatch ambulances. Estimates for emergency response time is 8-10 minutes. Fire hydrants are available in the office park.

The nearest hospital with an emergency room is 5 miles away.

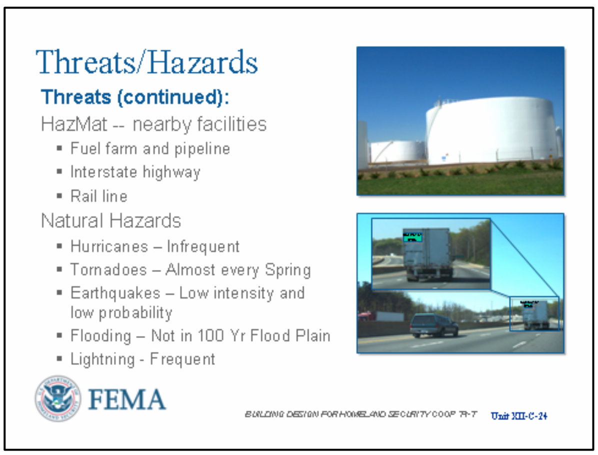
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-23

Threats/Hazards – Terrorism, Intelligence, and Crime

- Terrorism – no direct threat, but collateral damage possible
- Intelligence – due to work done by CI/BC this is always a concern
- Crime – relatively low for the type of work being done

VISUAL XII-C-24



Threats/Hazards – HazMat, Technological, and Natural

Many forms of HazMat in the local area, but especially the Tank Farm and the Interstate Highway are potential locations for Technological Hazards (accidents)

Natural Hazards have also been researched, indicating that this COOP Alternate Facility is in a lower risk area than the DAI Primary Facility.

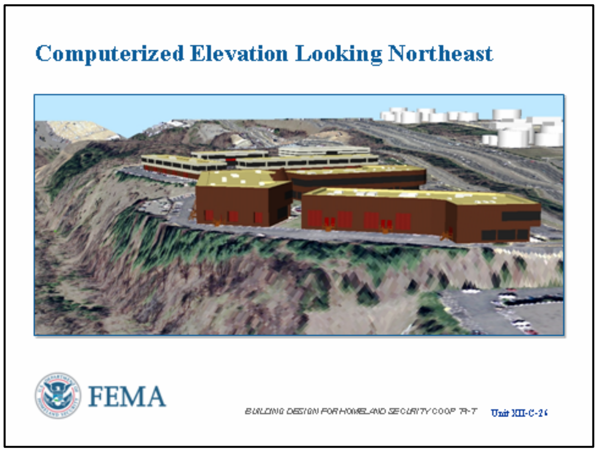
VISUAL XII-C-25

Elevation Looking Northwest

The lay of the land indicates that a fuel spill from the Tank Farm will not get to the CI/BC building, as well as any liquid spill on the Interstate Highway.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

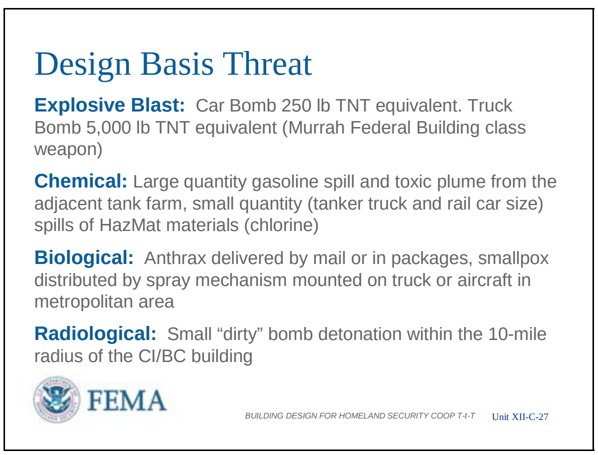
VISUAL XII-C-26



Elevation Looking Northeast

Similarly, along the back of the office park the terrain makes vehicle approach very difficult and liquid HazMat spills from the railroad line will not flow to the CI/BC building. The slope will also tend to direct any gases blown toward CI/BC from the southwest to be propelled up and over the CI/BC portion of the building.

VISUAL XII-C-27



Design Basis Threat

Explosive Blast: Car Bomb – approximately 250 lb TNT equivalent. Truck Bomb – approximately 5,000 lb TNT equivalent (Delivery Truck)

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

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

Radiological: Small "dirty" bomb detonation within the 10-mile radius of the CI/BC building.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XII-C-28

Levels of Protection

DHS Interagency Security Committee Criteria

Level II Building – between 11-150 employees; 2,500 to 80,000 sq ft

- Perimeter Security
- Entry Security
- Interior Security
- Administrative Procedures
- Blast/Setback Standards

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit XII-C-28

Levels of Protection -- DHS

DHS Level II Interagency Security Committee Criteria

- Perimeter Security
- Entry Security
- Interior Security
- Administrative Procedures
- Blast/Setback Standards

VISUAL XII-C-29

Levels of Protection

DoD Antiterrorism Standards

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Low	Moderate damage – Building damage will not be economically repairable. Progressive collapse will not occur. Space in and around damaged area will be unusable.	Glazing will fracture, potentially come out of the frame, but at a reduced velocity, does not present a significant injury hazard. (Very low hazard rating) Doors may fail, but they will rebound out of their frames, presenting minimal hazards.	Majority of personnel in damaged area suffer minor to moderate injuries with the potential for a few serious injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience minor to moderate injuries.

FEMA

FEMA 426, Adapted from Table 4-1: DoD Minimum Antiterrorism Standards for New Buildings, p. 4-9, updated for *UFC 4-010-01, 22 Jan 2007*

BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit XII-C-29

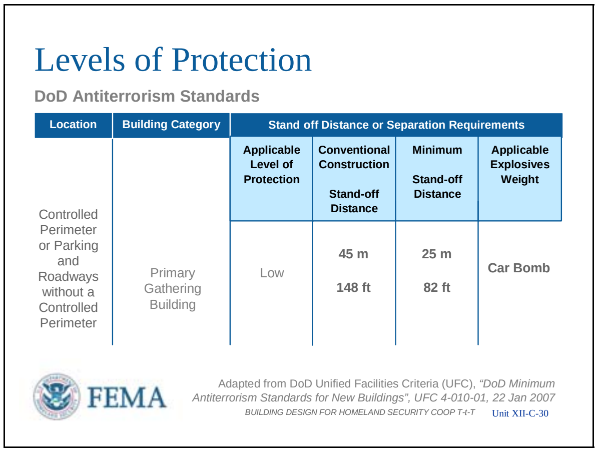
Levels of Protection -- DoD

DoD Low, Primary Gathering Building (more than 50 people regularly in structure)

- Potential Structural Damage
- Potential Door and Glazing Hazards
- Potential Injury

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-30



Levels of Protection

DoD Antiterrorism Standards

Location	Building Category	Stand off Distance or Separation Requirements: Applicable Level of Protection	Conventional Construction Stand-off Distance	Minimum Stand-off Distance	Applicable Explosives Weight
Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	Primary Gathering Building	Low	45 m 148 ft	25 m 82 ft	Car Bomb

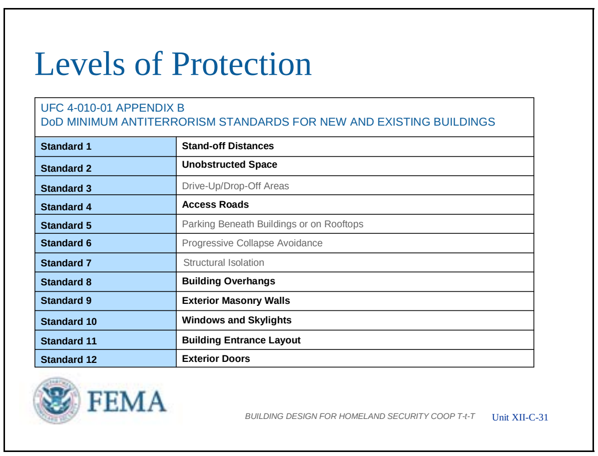
Levels of Protection – DoD (cont.)

DoD Low, Primary Gathering Building Stand-off Distance or Separation Requirements

This is WITHOUT a Controlled Perimeter where VBIEDs (Vehicle Borne Improvised Explosive Devices) would be detected.

NOTE to instructor: While this is one goal, having a Controlled Perimeter at the outer reaches of the parking lot reduces the stand-off distance for vehicles to 25m (82 feet) and 10m (33 feet) in the two respective columns.

VISUAL XII-C-31



Levels of Protection

UFC 4-010-01 APPENDIX B
DoD MINIMUM ANTITERRORISM STANDARDS FOR NEW AND EXISTING BUILDINGS

Standard 1	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 and Skylights
Standard 11	Building Entrance Layout
Standard 12	Exterior Doors

Levels of Protection

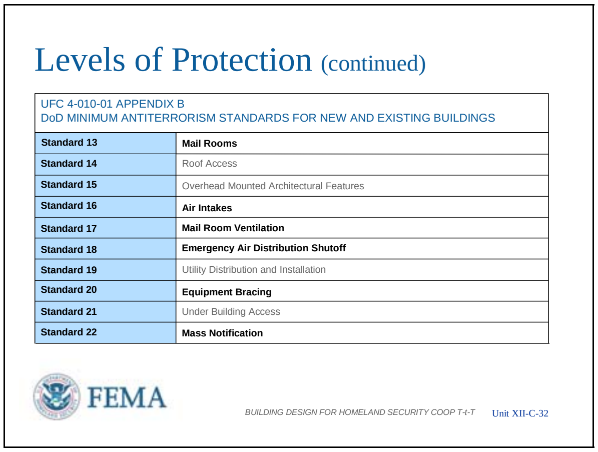
UFC 4-010-01 Appendix B
(22 January 2007)
DoD Minimum Antiterrorism Standards for New and Existing Buildings Standards 1-12

What standards are applicable to the Case Study?

- Std 1 – Stand-Off Distances
- Std 2 – Unobstructed Space
- Std 4 – Access Roads
- Std 8 – Building Overhangs
- Std 9 – Exterior Masonry Walls
- Std 10 – Windows and Skylights
- Std 11 – Building Entrance Layout
- Std 12 – Exterior Doors

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-32



Levels of Protection

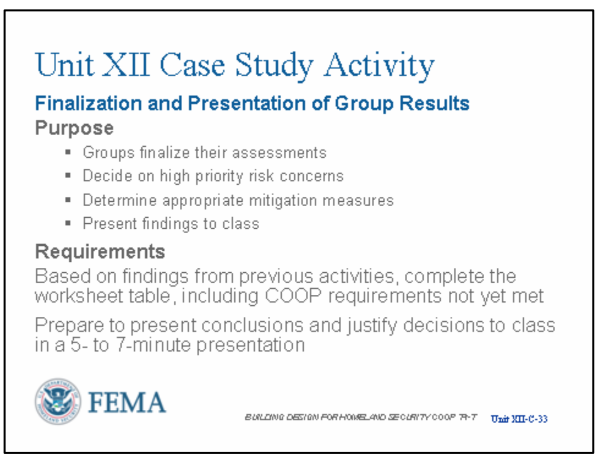
UFC 4-010-01 Appendix B
(22 January 2007)
DoD Minimum Antiterrorism Standards for New and Existing Buildings Standards 13-22

What standards are applicable to the Case Study?

- Std 13 – Mail Rooms
- Std 16 – Air Intakes
- Std 17 – Mail Room Ventilation
- Std 18 – Emergency Air Distribution Shutoff
- Std 20 – Equipment Bracing
- Std 22 – Mass Notification

In addition to the standards, review the DoD Recommendations for New and Existing Buildings, Appendix C.

VISUAL XII-C-33



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

At the end of 45 minutes, reconvene the class and facilitate group reporting.

Case Study Activity

In this unit, the students will finalize the assessment, determine high priority risk concerns, recommend appropriate mitigation options, and present findings to the class.

Activity Requirements

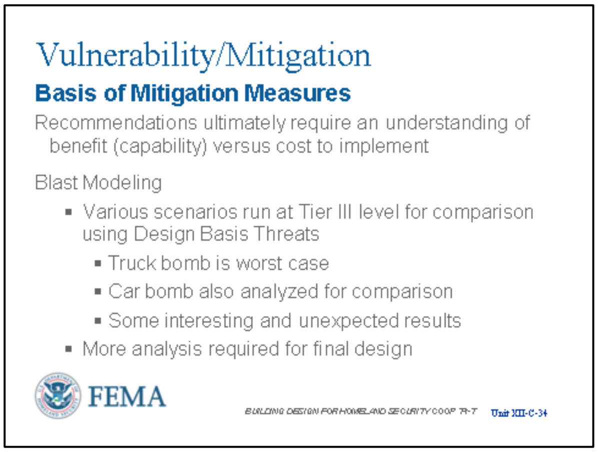
- Working in assessment groups, refer to the Case Study and imbedded GIS portfolio to determine answers to the worksheet questions.

- Then review results to identify vulnerabilities and possible mitigation measures, and rank and prioritize the findings.

- Additionally, refer back to the student activity for Unit I and identify all requirements gaps in the CI/BC building needed to meet COOP Alternate Facility FPC-65 criteria.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XII-C-34



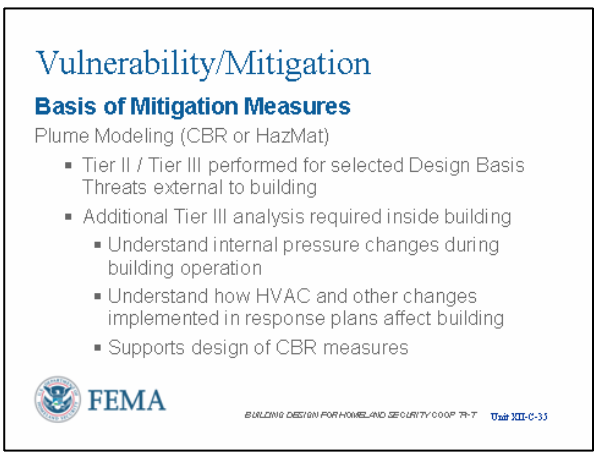
Vulnerability Mitigation – Basis of Measures - Blast

Need to understand benefit versus cost.

Blast modeling concentrates upon worst case, but must work all scenarios. Since both positive and negative blast wave phases are used in retrofitting existing buildings, results were interesting and, in some cases unexpected.

The higher tier assessment indicates the first cut of possible approaches, but more analysis is needed to work with the architects and engineers in achieving a final design.

VISUAL XII-C-35

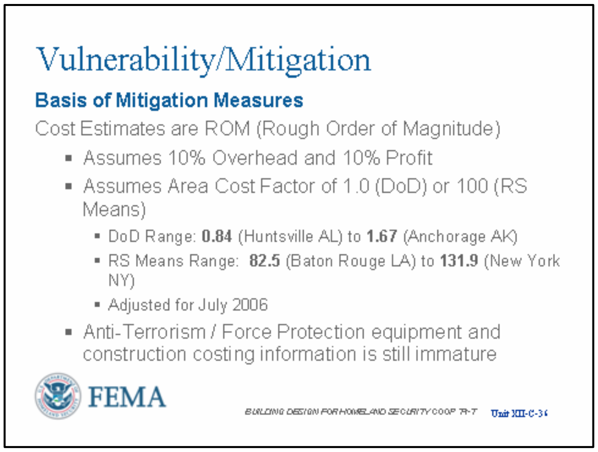


Vulnerability Mitigation – Basis of Measures - Plume

Plume modeling for CBR or HazMat follows similar approaches to indicate actions to consider, then followed by more detailed analysis to achieve the final design.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-36



Vulnerability Mitigation – Basis of Measures – Cost

When comparing benefit versus cost, the cost is equally difficult to determine due to the still immature nature of anti-terrorism / force protection costing information.

The costing used in this presentation assumes 10% overhead, 10% profit, an Area Cost Factor of 1.0, and adjusted for July 2006.

For your actual situation you can then adjust the dollar values given for your conditions.

VISUAL XII-C-37

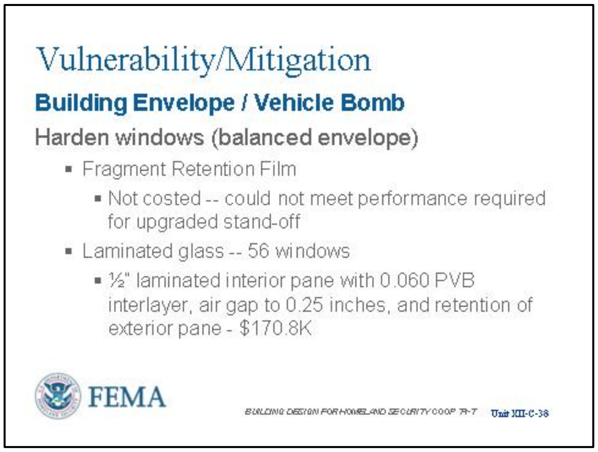
Vulnerability/Mitigation – Site / Vehicle Bomb

The front side and rear of the building have access roads that allow straightaway approaches to the building, especially the front. The achievable speed requires K12 stopping power.

For the front of the building, there are three options to hinder this approach and provide some stand-off to the situation. Landscaping using large boulders is the cheapest and has aesthetic qualities.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-38



Building Envelope / Vehicle Bomb

The windows are those found in standard commercial construction. They are relatively weak and require significant increase in tensile strength.

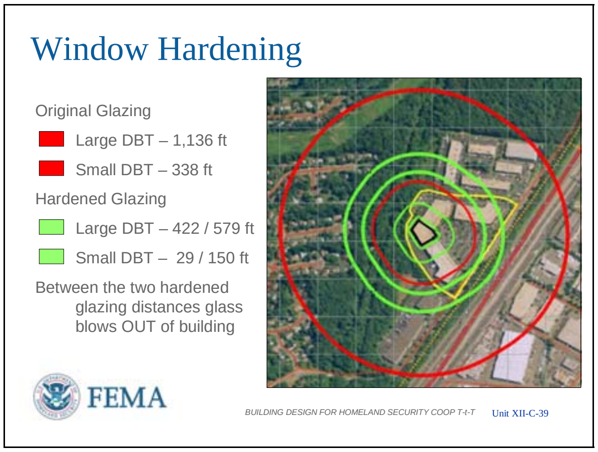
The goal is to achieve a balanced envelope between windows and walls.

While fragment retention film (FRF) comes to mind as the first glazing mitigation measure, it is not always successful in achieving protection for the existing stand-off available or the upgraded stand-off achieved through other measures. In this case 15 mil FRF requires 92 feet of stand-off for the Small DBT and is greater than 500 feet for the Large DBT. Thus putting a controlled perimeter on the main road outside the office park would not achieve protection from the Large DBT. And achieving 92 feet of stand-off from CI/BC will greatly impact parking at the office park, especially if the mitigation measure is extended to the other buildings in the office park.

Laminated glass with a 60 mil interlayer was selected for the interior pane so that the existing 1-inch IGU (insulated glass unit) frame could be reused to save money. This resulted in reducing the 1/2" air gap to 1/4" and retaining the exterior pane. This turned out to be the minimum upgrade for the projected controlled perimeter stand-off distance.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL XII-C-39



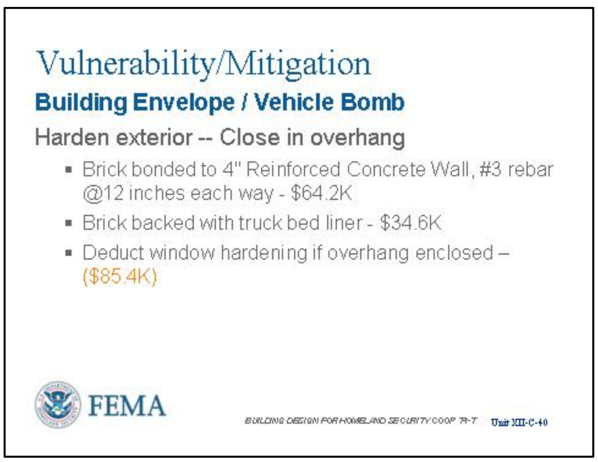
Window Hardening

As can be seen the Large DBT for the original glazing (thicker red contour) encompasses much of the interstate highway. The Small DBT (thinner red contours) covers a good portion of the parking lot.

The upgraded window with the 1/2" laminated glass inserted as the interior pane (and confirmation that the window frame connections to the building can survive the blast loading) reduces the stand-off to a controlled perimeter at the entrances to the office park for the Large DBT.

For the Small DBT, building occupants are protected down to a 29-foot stand-off. Although from 29 feet to 150 feet the glazing blows OUT of the building during the negative phase of the blast.

VISUAL XII-C-40



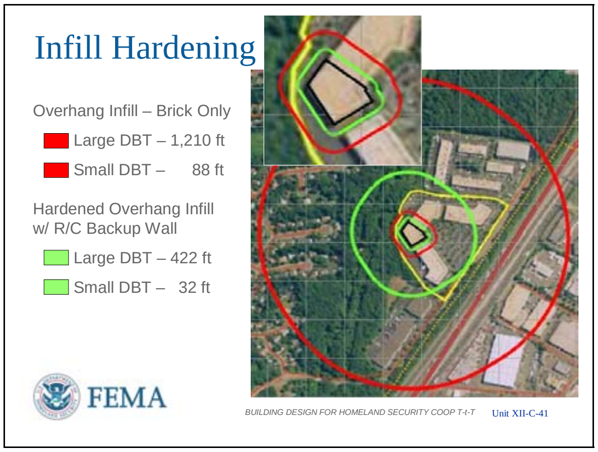
Building Envelope / Vehicle Bomb

Next, the goal is to enclose the overhang as this architectural feature greatly increases blast damage. Two mitigation options were analyzed. A benefit of enclosing the overhang results the savings indicated as half the windows in the CI/BC building would then not require hardening.

Note that brick is retained for architectural compatibility and the Spray-On Polymer (truck bed liner) is significantly cheaper than the reinforced concrete backing wall.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XII-C-41

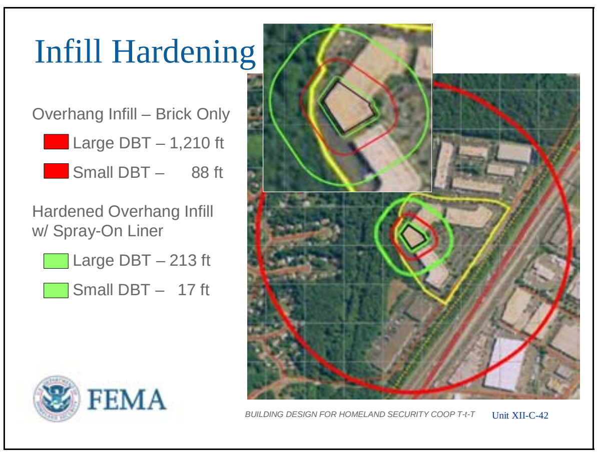


Infill Hardening – R/C Backing Wall

Comparing to a Brick Only wall (which is also an indication of the blast resistance of the outer wythe of the double wythe wall) shows that Brick is even weaker than the windows.

The reinforced concrete backing wall helps by keeping the Large DBT contour inside the main road serving the office park. The standoff for the Small DBT also has limited impact on changing parking in front of the CI/BC building.

VISUAL XII-C-42



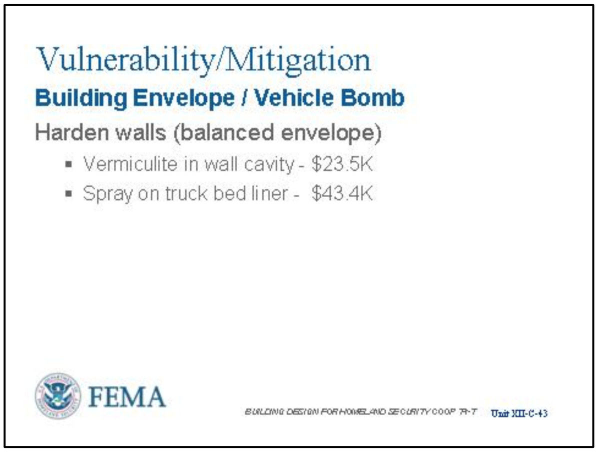
Infill Hardening – Spray-On Polymer Liner

The performance of the truck bed liner is remarkable considering it is only 1/4” thick with a 1 foot overlap onto the concreter overhang ceiling and the concrete overhang floor.

The Spray-On Polymer Liner shows about half the stand-off distance compared to the R/C Backing Wall, and, since it is cheaper, then it is the preferred mitigation measure. Be aware that the Spray-On Liner has some environmental concerns during installation and fire concerns due to its fuel capacity.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XII-C-43



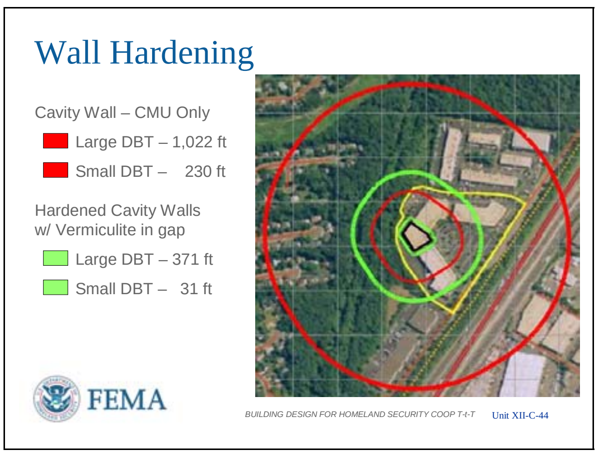
Wall Hardening

The cavity wall (Brick / Cavity / CMU) gains strength if both walls act together to resist the blast pressure vice working independently like tearing individual pages of a phone book to tear a phone book in half.

The Vermiculite in the wall cavity has mechanical properties that supports the need to tie the two walls together so that they act as one.

The Spray-On Polymer Liner (truck bed liner) is expected to have good performance per the Infill Hardening just presented, but at almost twice the cost of the Vermiculite. The exterior walls must be stripped to the CMU surface for applying the Liner, and then wallboard has to be replaced.

VISUAL XII-C-44

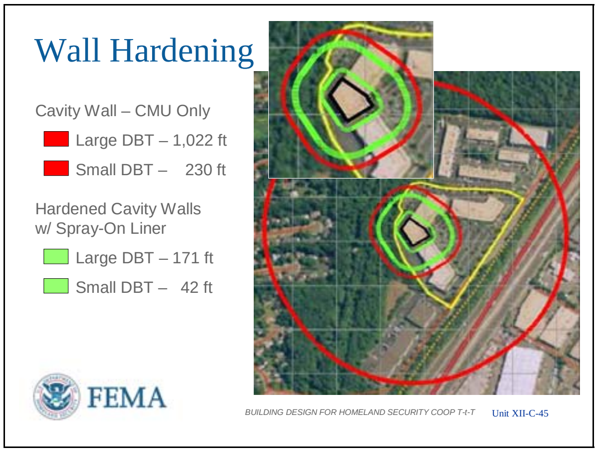


Wall Hardening – Vermiculite

The Vermiculite provides comparable stand-off to that needed for retention of parking and using the entrances to the office park as the controlled perimeter access control points.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

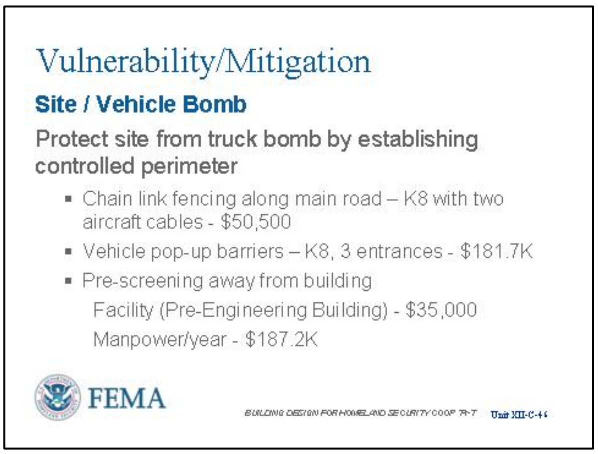
VISUAL XII-C-45



Wall Hardening – Spray-On Liner

As expected, the Spray-On Polymer Liner has very good performance, especially for the Large DBT. However, the controlled perimeter location and the additional cost of the Liner, justifies going with the Vermiculite to achieve a balanced envelope.

VISUAL XII-C-46



Site / Vehicle Bomb

Establishing a controlled perimeter is the next step (but should be started first as it affects all the other office park tenants).

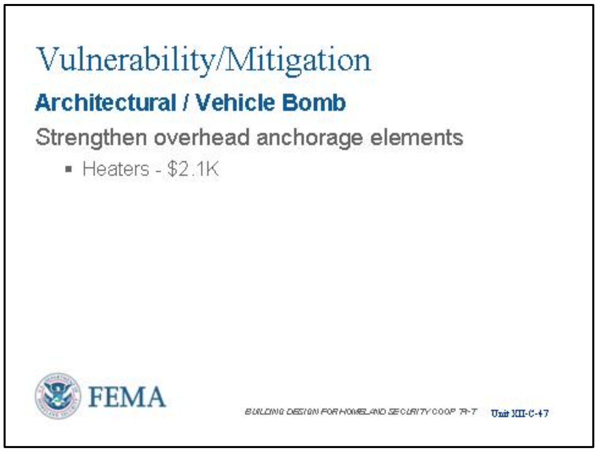
K8 ratings along the main road will provide the level of protection needed with three entrances as follows:

- Truck entrance
- Car entrance
- Truck exit (one-way traffic flow with trucks only allowed on the back side of the office park buildings.

If screening is not done at the vehicle entrance, then pre-screening off-site will be very expensive comparatively with a facility and annual labor. Access control can be by tenant with scheduled deliveries and remote control barrier operation linked with CCTV.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

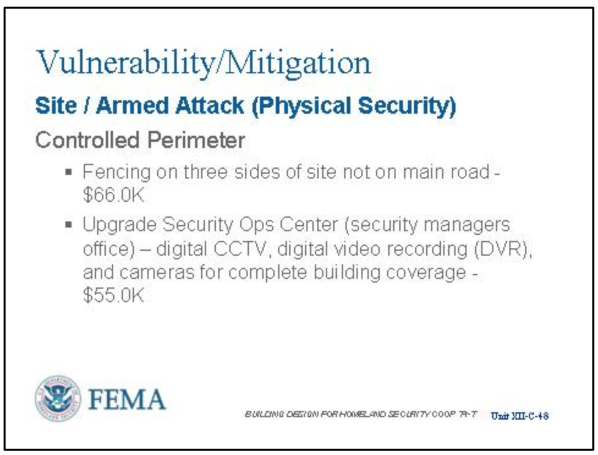
VISUAL XII-C-47



Architectural / Vehicle Bomb

A low cost mitigation measure is to upgrade the supports for the overhead heaters the areas near the loading dock per DoD guidelines.

VISUAL XII-C-48



Site / Armed Attack (Physical Security)

In addition to the controlled perimeter along the main road, upgrading the fencing around the back of the office park is also in order to control foot access

Upgrading the Security Operations Center with updated digital CCTV, digital recording, and cameras for complete building coverage would also be in order, in addition to vehicle access points.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

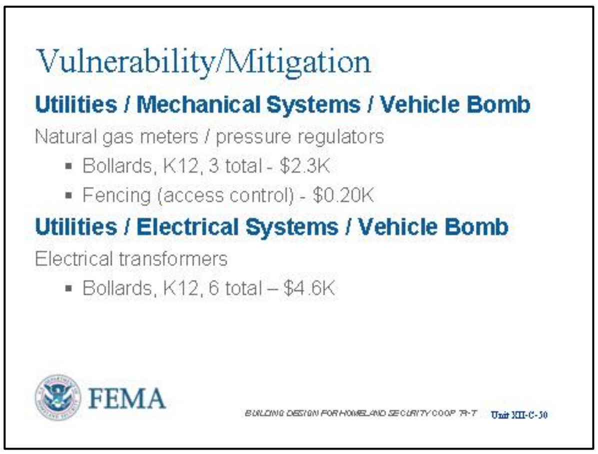
VISUAL XII-C-49

Architectural / Mailroom

Two approaches for the mailroom were considered:

- The first is to convert the receptionist lobby into a mailroom operation area (to continue using the receptionist as the mail clerk).
- The second is to build a separate mailroom, which will probably require someone else to perform mail duties.
- In either case, sealing, hardening, and separate HVAC are in order.

VISUAL XII-C-50



Utilities / Vehicle Bomb

Protection of utilities on the backside of the building also comes under the low cost umbrella. As stated previously the straightaway allows high-speed approach to the back of the CI/BC building. K12 fixed bollards and fencing to prevent approach to these systems needs consideration.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL XII-C-51

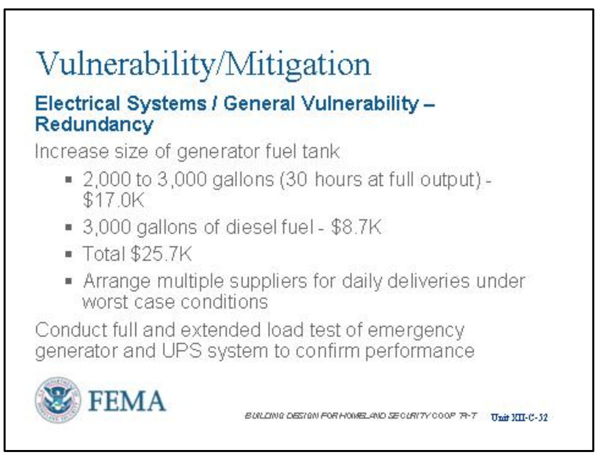
Mechanical / Fire / General Vulnerability - Redundancy

For better control of the Fire Alarm and Fire Suppression Systems, install a fire annunciator panel in CI/BC area of the building.

Rezone the fire alarms throughout the building and install dual zones in the Data Center to support adding the Clean Agent system in the Data Center (and probably the Communications Center). Note that depending upon local codes the Clean Agent system will NOT REPLACE the water sprinkler system.

The Chilled Water supply and return lines are vital to the proper operation of the Data Center. Adding redundant lines should be considered to maintain 24/7 operations.

VISUAL XII-C-52



Electrical / General Vulnerability – Redundancy

Since electricity is vital to 24/7 operations the existing 2,000 gallon fuel tank (and 250 gallon day tank) will not last long enough to maintain a once-per-day delivery schedule at full load (which may occur only during the heat of the summer). The generator consumes 100 gallons per hour. Replacing the fuel tank is one approach, or renting a fuel truck during the peak summer season when the 2,000 gallon fuel tank re has insufficient fuel capacity is another.

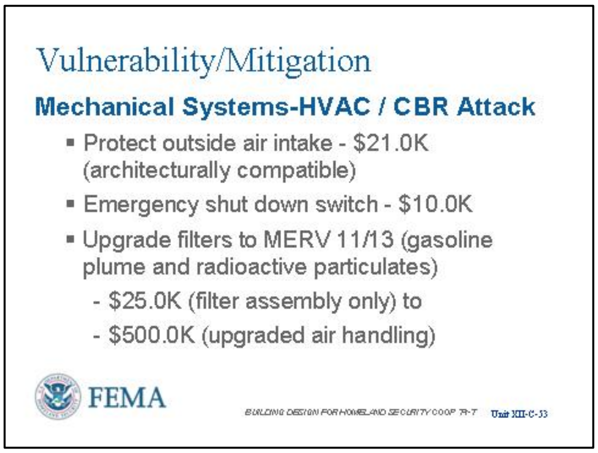
Multiple fuel suppliers should be arranged to prevent a single occurrence (like a utility power outage) from preventing deliveries or fuel supplies should be canvassed to determine if they have backup generators to overcome utility power outages.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Finally, upgrading the generator and UPS testing program is in order.

- Test the generator and outage sensor system once per month for 2 hours at the peak electrical consumption of the week.
- Test the battery capacity of the UPS once per year to ensure it can carry the load for the time required for orderly shutdown.

VISUAL XII-C-53



HVAC / CBR Attack

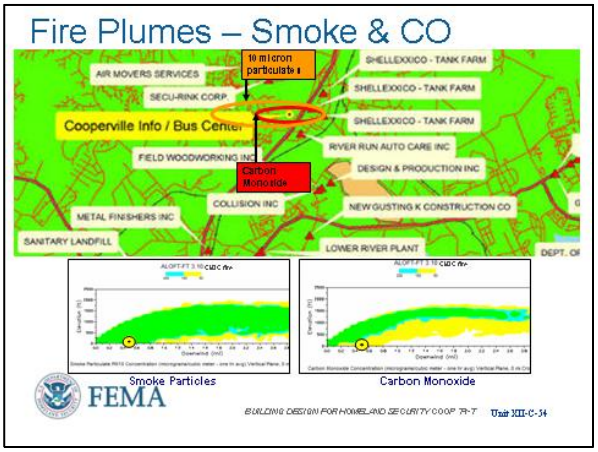
Raising the outside air intake is probable the first action to take to make it less vulnerable to attack and reduce the risk of heavier-than-air agents. This measure is more expensive because it will have to be architecturally compatibility (brick).

The second action is the emergency shutdown switch to shut down all air handling equipment in the building. If funds are tight, this should be the first action as it is less expensive than raising the air intake.

Upgrading the filters of the HVAC systems from MERV 8 to MERV 11/13 has a potential range of cost that requires further investigation. It is beneficial whenever there are particulates involved. It can be as simple as adding the filters or as expensive as upgrading the complete air handling system to accommodate the pressure drop of the higher MERV filters.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL XII-C-54



Fire Plumes – Smoke and Carbon Monoxide

Two points to consider are smoke particles that MERV 11.13 filters will capture and carbon monoxide, a lighter-than-air gas that kills by overcoming the oxygen in a room. The wind direction for this scenario does not follow the predominant wind patterns shown in earlier HazMat slides.

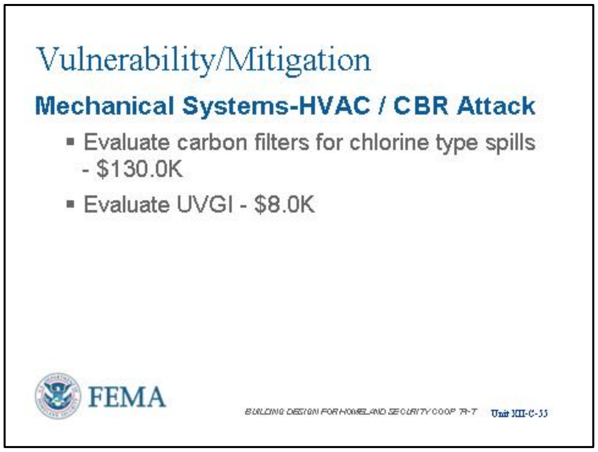
Circles on the lower graphs indicate the approximate location of the CI/BC building.

The smoke particles will be in high concentration as they reach the CI/BC building as shown in the lower left graphic. Filtering of these smoke particles is not only a concern from a human health standpoint, but also for sensitive electronic equipment, such as computer and communications.

Alternately, the carbon monoxide will be at a lesser concentration, but still high, although not high enough to be instantly fatal. This allows for evacuation from the site if a plume heads for the building. Sheltering-in-place is not recommended in this case.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL XII-C-55

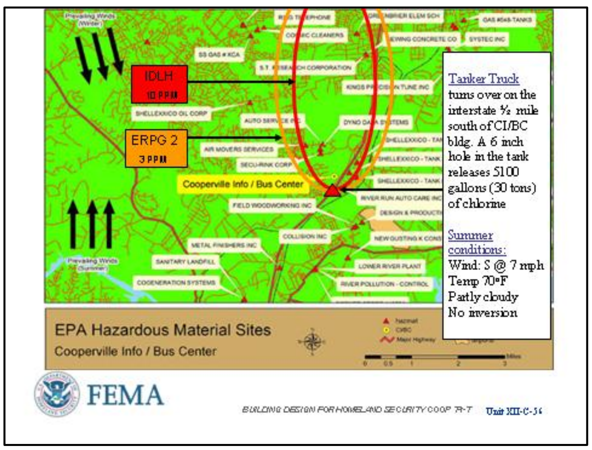


HVAC / CBR Attack

Carbon filters for removal of chlorine gas and similar gaseous spills is expensive and the filters should be on a sensor to switch them into the system when needed, rather than always being in operation – pressure drop and eventual consumption of capacity.

Ultraviolet Germicidal Irradiation (UVGI) in contrast is very reasonable and has the added benefit of killing biological agents in addition to standard infections. Thus, building air recirculation through the UVGI will not only protect from (C**B**R) attack, but has the capability of reducing employee downtime due to spreading normal diseases (flu, colds, etc.) through the air handling system.

VISUAL XII-C-56



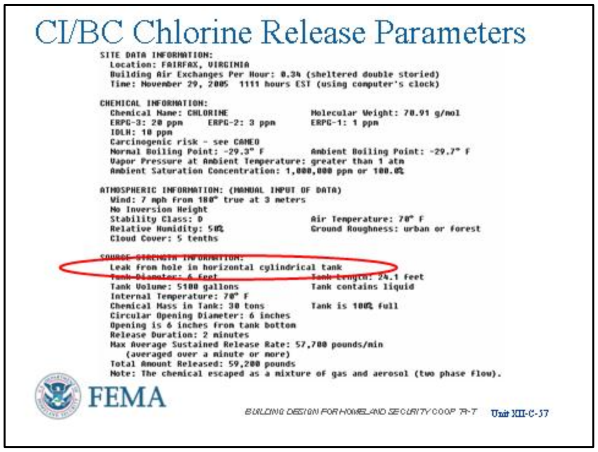
Chlorine Spill – Tanker Truck on Interstate Highway

In this case the prevailing winds are from the south, sending the chlorine plume over the CI/BC building.

- Immediately Dangerous to Life or Health (**IDLH**) refers to a concentration, formally defined as the maximum exposure concentration of a given chemical from which one could escape within 30 minutes without any escape-impairing symptoms or any irreversible health effects. The IDLH for chlorine is 10 ppm.
- The **ERPG-2** is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hr without experiencing or developing irreversible or other serious health effects or symptoms which could impair an individual's ability to take protective action.

INSTRUCTOR NOTES

VISUAL XII-C-57



CONTENT/ACTIVITY

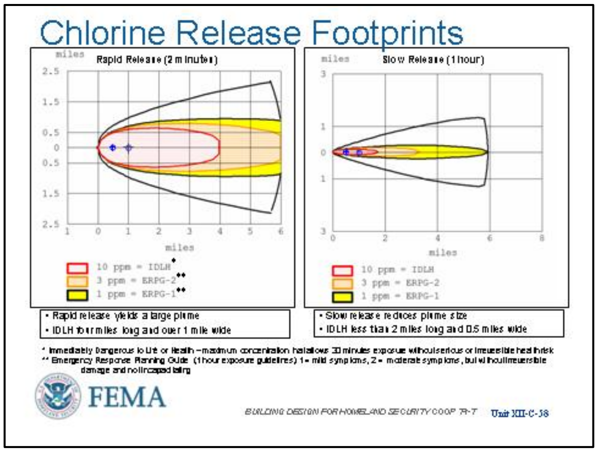
CI/BC Chlorine Release Parameters

This slide shows the information available from the CAMEO toxic industrial chemical (TIC) modeling program of EPA and NOAA and can be downloaded at http://archive.orr.noaa.gov/cameo/aloha.html.

- It is important to note that chlorine is approximately 2.5 times heavier than air so it will not readily disperse into the atmosphere. Instead it will hug the ground as it disperses and will settle in the lowest elevations.
- Notice this release is a rapid release of 5100 gallons (30 tons) of chlorine through a 6-inch hole in the tanker truck. The entire release occurs in approximately two minutes.
- A much smaller leak was also modeled (such as might occur in a ruptured hose) in order to demonstrate how changing just one variable makes a tremendous difference in the release and potentially in the response.

INSTRUCTOR NOTES

VISUAL XII-C-58



The **ERPG-3 (not shown)** is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hour without experiencing or developing life-threatening health effects.

CONTENT/ACTIVITY

Chlorine Release Footprints

On the left is a basic plume footprint for the rapid release of chlorine [5100 gallons (30 tons) at 225 psi over 2 minutes].

On the right is the footprint for a slower release, occurring over the course of one hour.

The blue circle with plus sign indicates the range of building location versus spill site (from 0.5 miles to one mile).

Note how a rapid release covers a much wider area, but reduces the DOSE (concentration x time) that can be received. Whereas the slow release is a bigger problem as a high concentration is present for a much longer time.

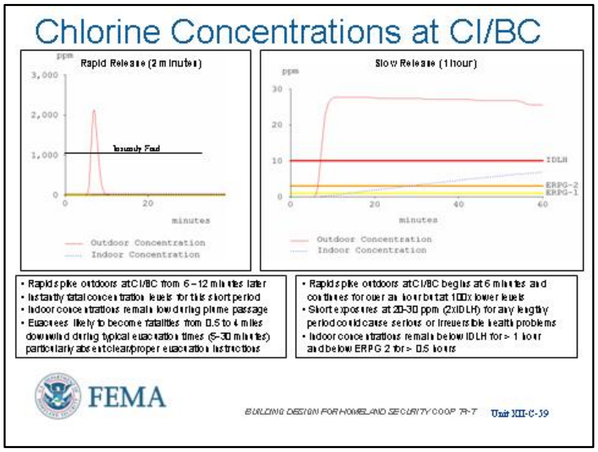
Immediately Dangerous to Life or Health (IDLH) [30 minutes] was defined earlier.

Emergency Response Planning Guides (ERPG) are defined in thin three categories

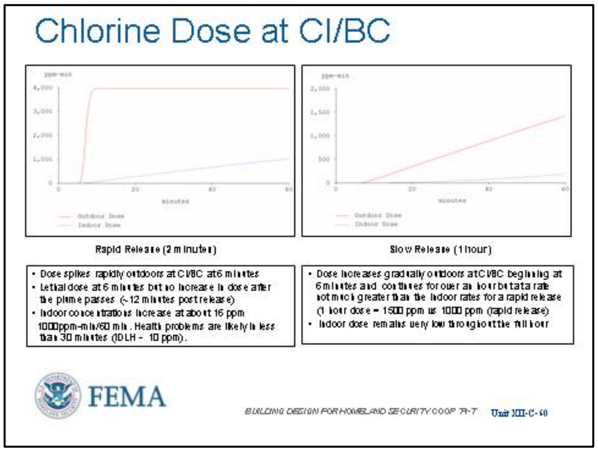
- The **ERPG-1** is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hr without experiencing other than mild transient adverse health effects or perceiving a clearly defined, objectionable odor.
- The **ERPG-2** is the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hr without experiencing or developing irreversible or other serious health effects or symptoms which could impair an individual's ability to take protective action.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL XII-C-59



VISUAL XII-C-60



Chlorine Concentrations at CI/BC

Bottomline: In all circumstances it is best to remain indoors unless or until the facts related to the release are clear and it can determined safe evacuation is possible. For even more protection move to upper floors and if intakes are roof-mounted - turn the HVAC on high (pressurize) until the odor of chlorine is noticed.

If configured, HVAC carbon filters can be put into operation or go to shelter-in-place configuration and turn on roof-mounted pressurization units.

Chlorine Dose at CI/BC

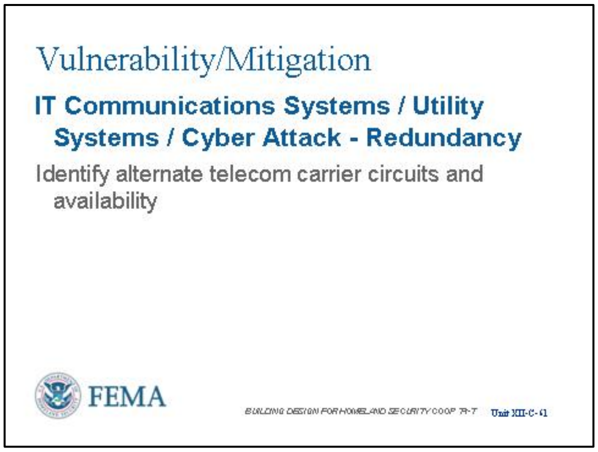
Bottomline: Once again it is clear that remaining indoors is the best option until or unless it is clear evacuation can be accomplished safely. It should be noted that the while the total indoor dose for the slow release is approximately **100 ppm-min** this only equals about 1.6 ppm (concentration) – well below IDLH and ERPG 2.

Any efforts to maintain a positive pressure in the building and seal exterior openings (particularly at the lowest levels) could further reduce the infiltration and therefore dosage for occupants.

After the plume passes, this would be the time to purge the building to reduce the indoor concentration and, thus reduce the dose to people inside the building. While high concentrations are a concern for immediate effects, high dosage is a concern for long-term effects.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XII-C-61



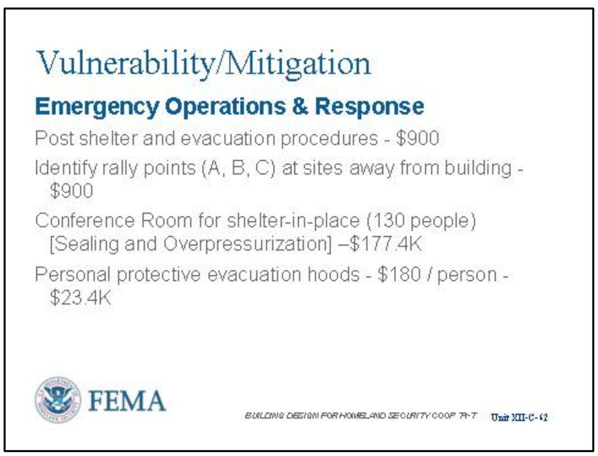
IT Communication Systems – Redundancy

Currently there is only one telecom carrier provider. Identifying an alternate telecom carrier and the availability of circuits that can be run to the CI/BC building provides similar backup as the generator and UPS provide to the electrical utility.

Since communications (data and voice) is so important to the CI/BC 24/7 operations, backup in this area should receive equivalent consideration.

NOTE: Since the CI/BC building needs a satellite communications link to satisfy DAI COOP requirements, this satellite link can provide the redundancy sought here.

VISUAL XII-C-62



Emergency Operations and Response

Low cost, no cost actions, especially shelter, evacuation, and rally point procedures should be the first step. And these should be updated as the building is reconfigured for updated operations.

For sheltering-in-place the conference room will require 3 filter/pressurization units on the roof to overpressurize the Conference Room. This will allow a longer shelter-in-place strategy, but NOT at a low cost.

Protective evacuation hoods are cheaper than overpressurization systems, but may not work with all agents with which personnel may contend. Recommend labeling the evacuation hoods for their design contaminants (or label them for the NON-DESIGN contaminants, whichever list is smaller).

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Transition

This completes the Building Design for Homeland Security instruction. In this course, you have learned how to perform a multihazard risk assessment of a building and have become familiar with the key concepts of how to protect buildings from manmade threats and hazards:

- Asset Value
- Design Basis Threat
- Levels of Protection
- Layers of Defense
- Vulnerability Assessment
- Risk Assessment
- Mitigation Options

Using the approach and guidance provided in **FEMA 426 / FEMA 452**, the majority of building owners should be able to complete a risk assessment of their building in a few days and identify the primary vulnerabilities, mitigation options, and make informed decisions on the ability of their building to survive, recover, and operate should an attack or event occur.

The next instruction unit will cover how to teach this course by covering basic Train-the-Trainer concepts and the support requirements for this course.

UNIT XII (C) CASE STUDY ACTIVITY: PREPARATION AND PRESENTATION OF GROUP RESULTS (COOP Version)

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

The student presenter(s) will decide on the number of asset-threat/hazard pairs to present and the mitigation measures to apply. Of great importance is the rationale for the selection of these high risk asset-threat/hazard pairs and the rationale for the recommended mitigation measures. No Cost / Low Cost recommended mitigation measures are always welcome as procedural changes can derive significant benefit.

In light of limited resources that building owners / decision makers have to work with, the presenter(s) will identify the top three asset-threat/hazard pairs that their assessment identified and the top three mitigation measures that they would recommend to have funded using those limited resources.

Since this facility is also being assessed for COOP capability to support the Federal Agency, identify any requirements that are not currently present in the CI/BC building.

Requirements

Activity #1: Based on findings from the previous activities and understanding of course content, complete the Assessment Team Briefing Summary table on the next page. One entry is provided as an example. Add at least three additional entries. Identify the <u>top three risks</u> and the <u>top three mitigation measures.</u>

Activity #2: Complete the COOP Requirements Gaps table for all COOP requirements gaps identified and recommendations to satisfy / correct them. This table is at the end of this Student Manual Unit.

Activity #3: Select one or two presenters from the assessment team to brief the team's conclusions and recommendations with rationale and justifications. The presentation should be 5-7 minutes in length. Ensure points in activities above are covered.

Assessment Team Briefing Summary

Prioritized Asset-Threat/Hazard Pair	Requirements to Mitigate	Rationale
Priority #: __________ *Envelope Systems / Vehicle Bomb*	*Protect building and internal functions and infrastructure from explosive blast.* *Priority #: __________* *1. Use planters, plinth walls, landscaping and / or reconfiguration of parking to increase standoff.* *Priority #: __________* *2. Harden glazing with Fragment Retention Film on windows or replace with laminated glass as this is the weakest exterior component.* *Priority #: __________* *3. Harden walls by installing vermiculite between wythes so they function as a single system.* *Priority #: __________* *4. Reduce reflective blast pressure by approaching property manager about closing in overhang area.*	Design basis threats include car bomb and truck bomb, with truck bomb more difficult to mitigate • Apply known standards, such as ISC Level II Blast/Setback Standards or DoD Standards 1,8, 9 and 10 / Recommendation 17 • Note that known standards are based upon a design basis threat that may or may not equate to design basis threat selected for the assessment • Increasing stand-off will reduce blast pressure and hardening will reduce blast pressure damage. Enclosing the overhang will significantly reduce reflective blast pressure on the first floor front side. • Fragment retention film can be selected to reduce summer heat gain to reduce air conditioning load. • Vermiculite can add to insulation factor of walls to reduce heating and cooling load on the building.

Prioritized Asset-Threat/Hazard Pair	Requirements to Mitigate	Rationale

***NOTE** to instructor: Due to the variations possible in student responses, there is no benefit in trying to prioritize the mitigation measures identified on pages IG XII-C-21 to IG XII-C-37.*

Referring back to Unit 5, Risk Assessment / Risk Management the following school solution high risks were identified.

***Risk #1**: Cyber Attack upon IT/Communications (630 / 576)*
***Risk #2**: Vehicle Bomb upon Data Center and Communications (480 / 432), but all Functions and Infrastructure is High Risk*
***Risk #3**: CBR Attack upon Data Center, Communications, Engineering/IT Technicians, and Mechanical Systems (320 / 288 / 256)*

Risk #1, Cyber Attack upon Communications, requires specialty personnel that are not specifically building oriented in their needed approach. However, building officials need to understand how this risk interfaces with the building.

Risk #2 and Risk #3 cover most of the mitigation measures identified on the pages mentioned (C-21 to C-37) above as these are the measures that apply to the building and site as designed and constructed.

COOP Requirements Gaps

COOP Requirement Gap	Action to Correct

UNIT XIII TRAIN-THE-TRAINER

TIME: 1 Hour

OBJECTIVES

At the end of this session, participants will be able to accomplish the following:

1. Discuss basic adult learning principles as they apply to participants in *Building Design for Homeland Security*.
2. Explain the key functions of instructional delivery as they apply to *Building Design for Homeland Security*.
3. Describe the key steps of instructional preparation as they apply to *Building Design for Homeland Security*.

OBJECTIVES

This unit covers the following topics:

1. Learning styles and preferences, characteristics of adult learners, adult learning assumptions (experience, motivation, active participation, and variety)
2. Adult training methodologies used in *Building Design for Homeland Security*
3. Steps for instructional preparation, preparing the environment, preparing yourself, and expecting the unexpected

INSTRUCTIONAL METHOD

The instructor introduces the unit and the unit references. The first part of the unit discussion addresses adult learning principles and preferences. If time allows, participants complete a brief self-assessment of their own adult learning styles and preferences; otherwise, the instructor refers to the inventory and suggests completion later. The instructor describes instructional methodologies that enhance learning for different styles and preferences, and engages participants in discussion about their own best learning environments and methods. The topic of the discussion is transitioned to the specific methodologies used in the *Building Design for Homeland Security Course*, and how they have been designed to reach the full spectrum of adult learning styles. Time allowing, the instructor provides additional tips for successfully employing the course's instructional methods.

Course preparation is the next topic of discussion. The instructor facilitates plenary group discussion about what is required of instructors to prepare to conduct the course. The instructor refers participants to the list of logistical details that must be completed to ensure the success of the training, and briefly reviews the requirements. The unit is concluded with a question-and-answer session to address any participant concerns or confusion.

SUPPLIES AND EQUIPMENT

The following are required for this unit:

- Chart paper, easel, and markers
- Course Instructor Guide
- Handout: “Preparing to Train Adults” (one per participant)
- Post-It® notes and highlighters
- Unit visuals in PowerPoint format, computer, LCD projector, and screen

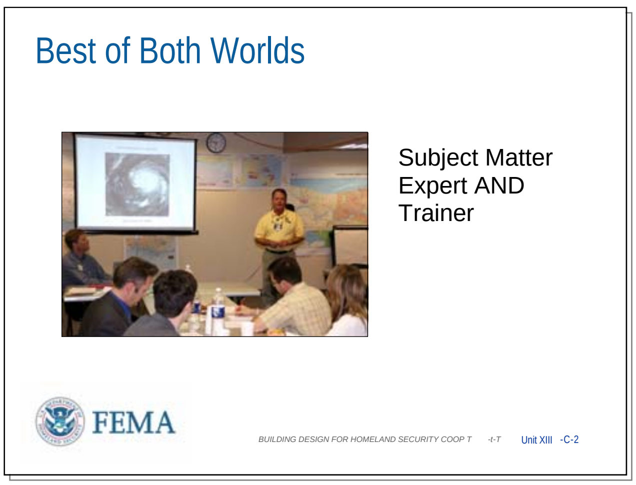
SUGGESTED TIME PLAN

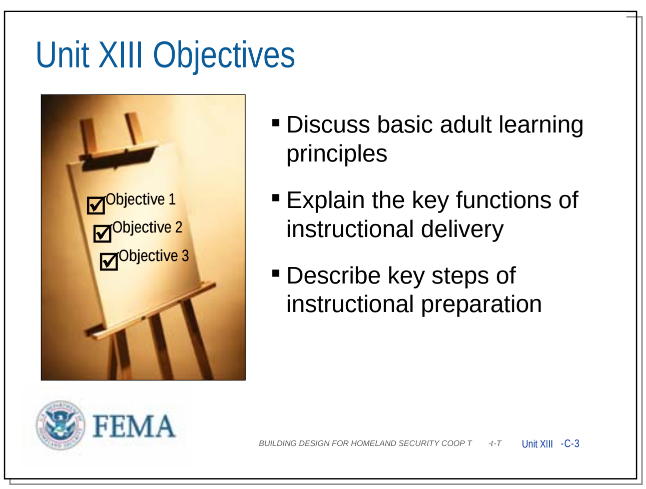
The following time plan is suggested for this unit:

Topic	*Time (Minutes)*
Introduction	3
Adult Learning Principles	15
Instructional Delivery	15
Course Preparation	15
Expecting the Unexpected	12
Total Time	60

Introduction

TIME: 3 Minutes





Introduction

Technical courses require thorough knowledge of the subject.

- Most of you are subject matter experts; may not have as much experience as trainers.

The purpose of this unit is to briefly touch on some basic principles of adult education and how to apply to teaching this course material.

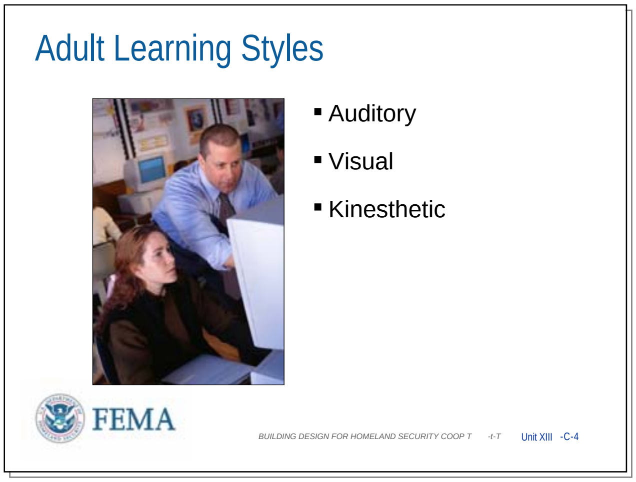
- Another purpose is to discuss logistical details of conducting this course.

Unit XIII Objectives

1. Discuss basic adult learning principles as they apply to participants in *Building Design for Homeland Security*.
2. Explain the key functions of instructional delivery as they apply to *Building Design for Homeland Security*.
3. Describe the key steps of instructional preparation as they apply to *Building Design for Homeland Security*.

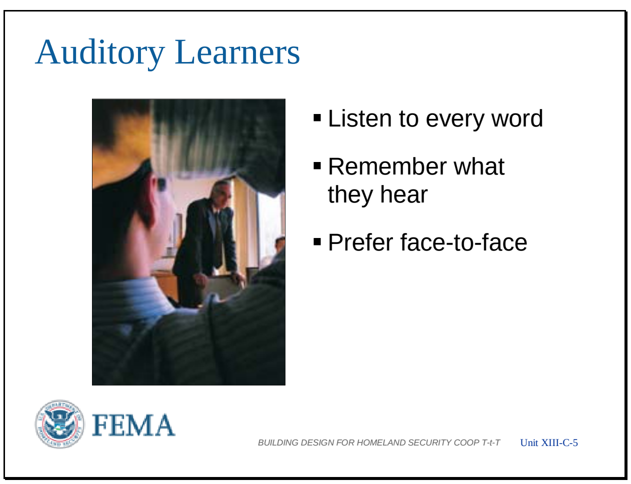
Adult Learning Principles

TIME: 15 Minutes



Refer participants to "Preparing to Train Adults" in Unit XIII of their Student Manual.

If time allows (approximately 15 minutes) have them complete this inventory in class.



Adult Learning Principles

Adult Learning Styles

If you want your training to make an impact, it needs to capture your learner's attention and interest.

To increase the chances that your information is well received and absorbed, you should try to match how you deliver the information as closely as possible to the learning styles of your audience.

The best way to understand learning styles is to understand your own preferences.

- If you want to know your own learning style, complete the Learning Preference Inventory on page 27 of "Preparing to Train Adults."

Auditory Learners

Auditory learners will listen to every word you say and will not write much.

- They learn best by hearing, seeing, and saying words.
- Written handouts are more meaningful to them if they are read out loud.
- They are good speakers and easily remember what they hear.

They prefer face-to-face or phone communication, so if you are trying to conduct pre-course work with them, you may have more difficulty interacting with them via e-mail or memos.

Mnemonic devices work well to reach auditory learners.

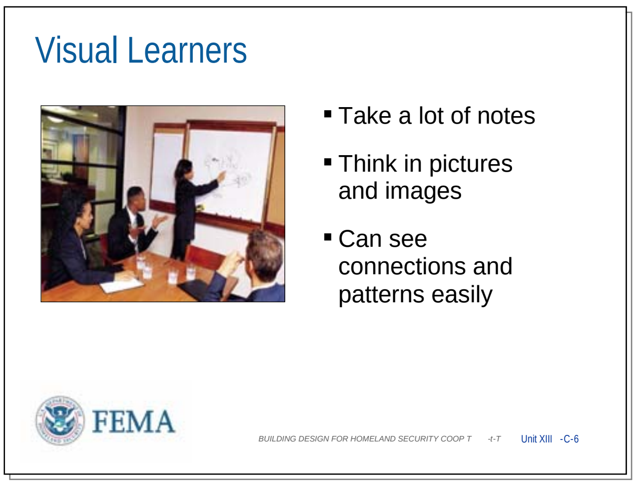
- These devices are words that link to other information (i.e., Every Good Boy Deserves Fudge for musical notes).

DISCUSSION QUESTION

Ask the adjacent question and solicit participant response.

DISCUSSION QUESTION

For the auditory learners in the class, are there any other "tricks" you use to help you learn or remember?



Visual Learners

Visual learners take a lot of notes and will try to capture everything in writing.

They think in pictures and images and are skilled at seeing connections and patterns in what is presented.

The visuals in your course materials, i.e., PowerPoint visuals, pictures, maps, videos, and graphs will appeal to your visual learners.

DISCUSSION QUESTION

Ask the adjacent question and solicit participant response.

DISCUSSION QUESTION

For the visual learners in the class, what else helps you learn or remember?

Kinesthetic Learners

Kinesthetic learners are hands-on learners.

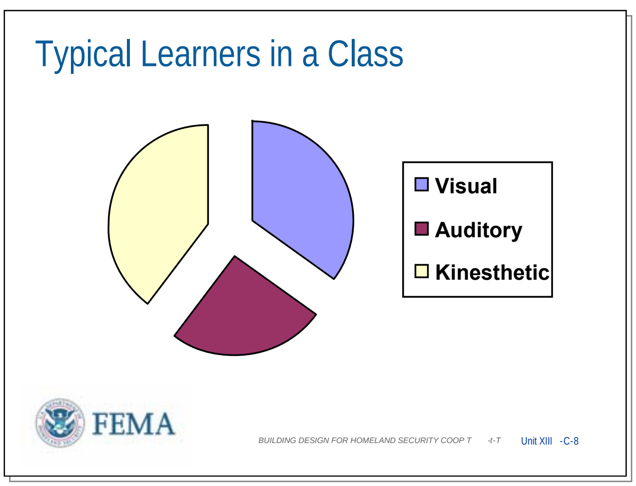
- They learn best by touching and doing.
- They like games, role-plays, and exercises.
- They can work in busy, noisy surroundings without getting distracted.

DISCUSSION QUESTION

Ask the adjacent question and solicit participant response.

DISCUSSION QUESTION

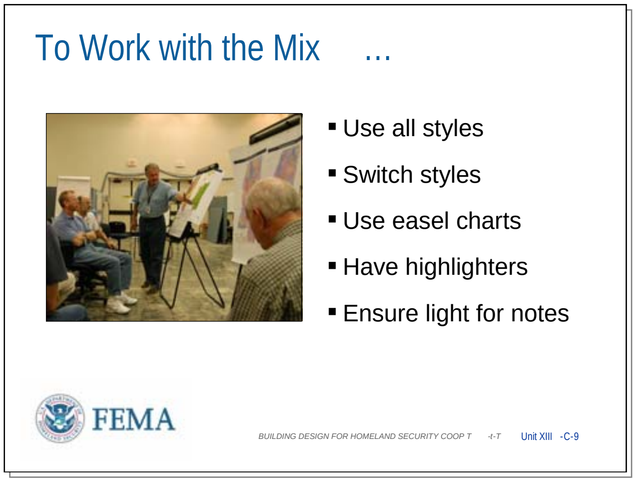
What other suggestions do the kinesthetic learners in the class have for helping hands-on learners?



Typical Learners in a Class

There is an average percentage of each type of learner in a typical class:

- Visual Learners: 30-40%
- Auditory Learners: 20-30%
- Kinesthetic Learners: 30-50%

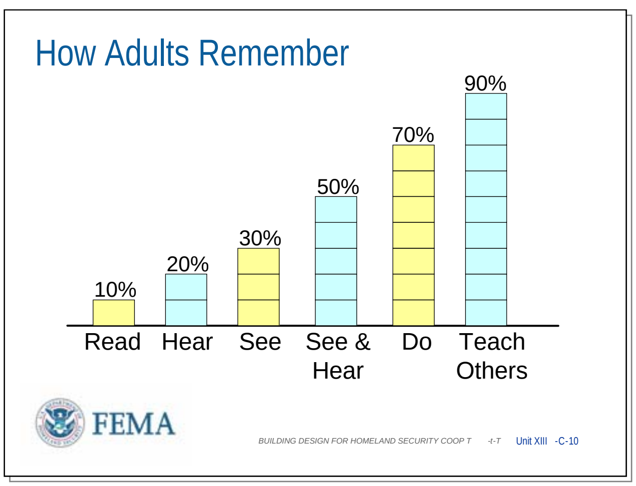


To Work with the Mix…

Be careful to use all styles so you do not become biased towards overusing your own style.

- Switch styles so that you are explaining concepts in words, using visuals, and practicing concepts through games, role-plays, and other activities.
- Track main points by using easel charts for the visual learners.
- Put highlighters on the table for the kinesthetic learners.
- Make sure there is enough light in the room for the note takers.

Watch your participants and, if you seem to be losing them, you may need to vary your style to get them re-engaged.

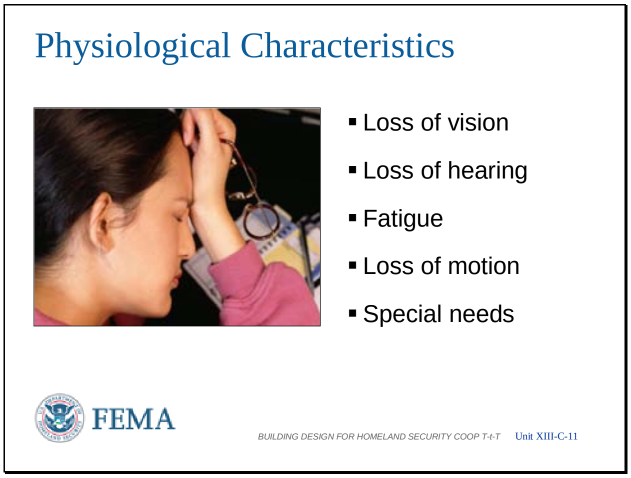


How Adults Remember

Adult learners are much more oriented to learning by sight than by hearing.

Learning by doing is the most effective for adults.

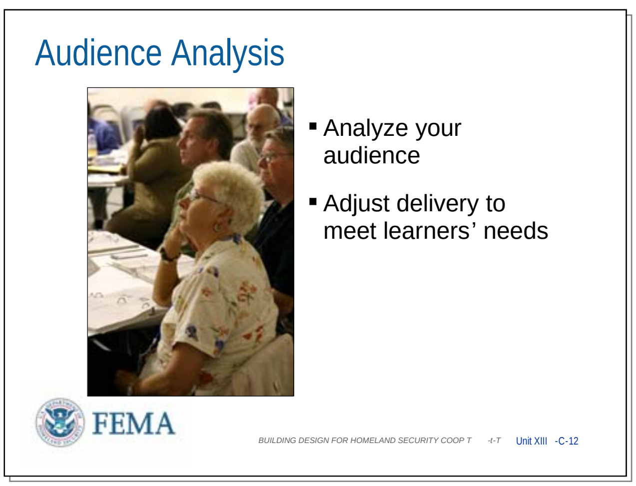
It is helpful to place written information in the hands of the participants to support areas of discussion.



Physiological Characteristics

Remember the possible physiological characteristics which may affect learning.

- Large font size should be used on projections, charts, and handouts.
- Hearing may also be a problem, so minimize background noise, check volume on recordings, and concentrate on good voice projection.
- Do not hesitate to use a microphone if one is available.
- Sensory impairment, such as poor vision or hearing loss, can restrict sensory input.
- Stress can impair memory.



Audience Analysis

DISCUSSION QUESTION

Ask the adjacent question and solicit participant response.

DISCUSSION QUESTION

How can you gather information about your audience?

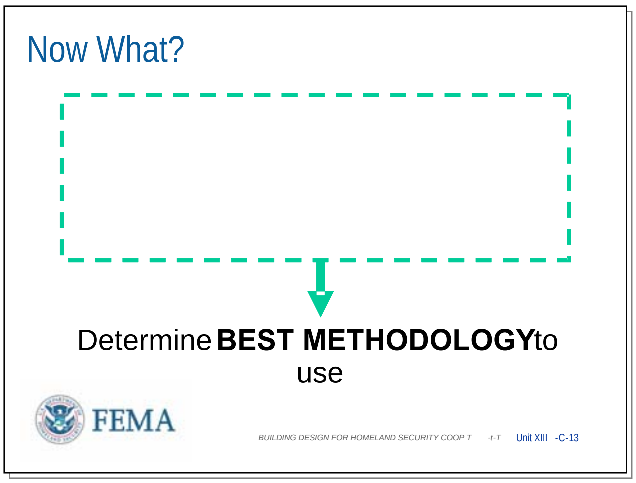
Suggested responses:

- *Review the roster*
- *Pre-course questionnaire*
- *In-class introductions*

The information obtained will enable you to match your delivery as closely as possible to the learner's needs to make last-minute adjustments, as needed, to how you teach *Building Design for Homeland Security.*

Instructional Delivery

TIME: 15 Minutes



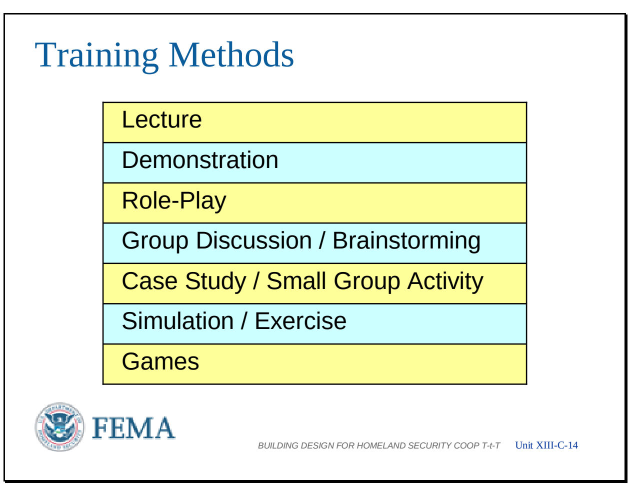
Instructional Delivery

Based on your audience analysis information, and given what you know about how adults learn, you can determine the best methodology for engaging your audience as well as which methodologies may be more difficult.

Building Design for Homeland Security has well-defined methodologies that should be carefully followed.

However, depending on your audience, one class may be more likely to ask questions and participate in discussions, while another class may be primarily visual learners.

If the class is experienced and mostly kinesthetic and oral learners, they will jump right into the exercises… another group may be less enthusiastic and need more encouragement.



Training Methods

These are different methodologies designed to fulfill specific learning objectives and to appeal to different types of learners.

DISCUSSION QUESTION

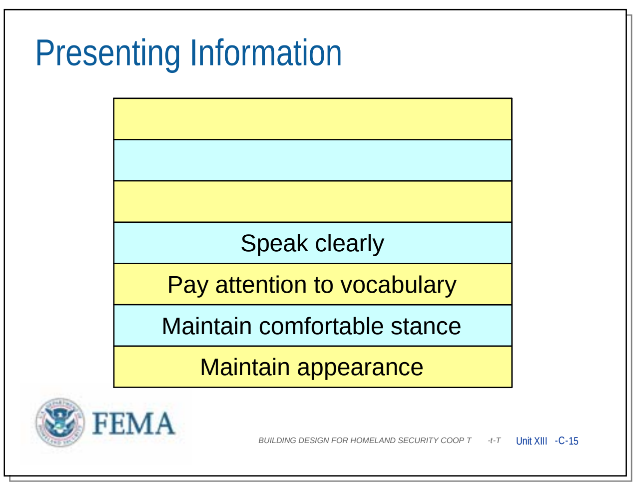
Ask the adjacent question and solicit participant response.

DISCUSSION QUESTIONS

Which ones are used in Building Design for Homeland Security?

Suggested responses:

- *Lecture*
- *Group Discussion*
- *Case Study*
- *Small Group Activity*
- *Role Play*



Presenting Information

Watch Your Body Language

- Use natural gestures to emphasize key points.
- Avoid distracting gestures (e.g., jingling change in your pocket).
- You want your body language to appear positive and open.

Maintain Eye Contact

- Position your body to face the majority of the audience.
- Move from behind the podium and walk toward the audience.
- Don’t read from your notes and lose eye contact all together.

Tone, Inflection, and Pace

- Vary your inflection to emphasize important words and messages.

- Speak more slowly than you would in normal conversation.
- Set your pace according to the audience's familiarity with the topic.
- For the first time you teach a section or topic, estimate how much time you need and then add 25 percent.
- Always end sessions and breaks on time.

Speak in Clear Sentences

- Vary your rate of speed to avoid sounding monotonous.
- Articulate sounds for clear pronunciation.
- Avoid um's and uh's – if you feel you are about to say "um," take a breath.
- Also watch the classic "you know."

Pay Attention to Vocabulary

- Be clear – match the language to the understanding level of your audience.
- Be colorful – use imagery to create a vivid picture of your information.
- Be concrete – avoid language that is vague or too general.
- Be concise – use short sentences that are easy to understand.
- Be correct – use consistent terminology and avoid slang.
- Do not use acronyms.
- Avoid heavy statistics.
- Use "you" a lot to build rapport with the audience.

Maintain a Comfortable Stance

- Don't block the audience's view.
- If using handouts only and everyone is

seated, also sit and face the audience.

- Move about the audience.

Avoid

- Moving around too much
- Rocking
- Slouching
- Overdoing or exaggerating anything

Think About your Appearance

- Wear clothes appropriate for your audience.
- When selecting colors and patterns, remember:
  - Cool/pastel colors have a calming effect.
  - Earth-tone colors communicate sincerity and genuineness.
  - Red denotes power.
  - Navy/dark blue denotes authority.
  - Avoid other bright colors or loud patterns.

Course Preparation

TIME: 15 Minutes

Preparing for Training: Course Materials

- Obtain Course CD from Eric Letvin (Visuals, Instructor Guide, Student Manuals)
- Print Instructor Guide(s) and Student Manuals in color
- Make copies of Student References CD and FEMA 452 Risk Management Database CD
- Obtain copies of FEMA 426 and FEMA 452 from Mila Kennett

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T -t-T Unit XIII -C-16

Preparing for Training: Preparation

Instructor Preparation

- Study Instructor Guide
- Send pre-course information to participants
- Form participant teams

Participant Preparation

- Download, print, and read case study from: http://www.fema.gov/plan/prevent/rms/rmsp155.shtm
- Bring laptop to download FEMA 452 Risk Assessment Database

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY COOP T -t-T Unit XIII -C-17

The adjacent information is an excerpt from Your Guide to FEMA.

Even if participants received the document in DFTO training, it is important enough to review.

Course Preparation

Course Materials

If you plan to conduct the complete course, the first step is to get the current materials.

- The slide lists the current procedure.
- Eventually all of the materials will be available on the FEMA website.

Preparation

Participants are notified to bring a laptop computer (for which they have software loading rights) if they wish to download the FEMA 452 Risk Assessment Database with instructor assistance and participate in an orientation to the screens.

- The case study is located in an appendix to the Student Manual.

If the course will be conducted at a site other than EMI, the lead instructor coordinates with the point of contact for that offering to ensure that registered participants are informed by e-mail or letter to read the appropriate case study.

Participant Teams

Prior to the course offering, the lead instructor refers to the roster of enrolled participants (name, organization, job title, phone, and e-mail) to compose preliminary teams who will work together on the case study activities throughout the course.

- Ideally, teams have five to eight members, with seven being optimal.

Teams are intended to reflect the general participant profile in terms of organization, subdivision of that organization, current job, past experience, and other education/training.

- Ideally, no team includes two people from the same office, doing the same job with the same skills.

The intent is to intersperse security personnel, architects, engineers, planners, facility managers, etc., among the teams to obtain a broad range of perspectives during the case study activities.

Participant teams are refined after the participant introductions in Unit One.

Preparing for Training

Coordination and Agenda

- Decide who will conduct units.
- Prepare the agenda in cooperation with the course sponsor.

Course Materials

Make sure you have adequate copies of the course materials:

- Course Instructor Guide (IG), one per instructor
- Course Student Manual (SM), one per participant
- FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*
- FEMA 430, *Primer for Incorporating Building Security Components in Architectural Design*, one per instructor and one per participant
- FEMA 452 Databases CD, one per

instructor and one per participant

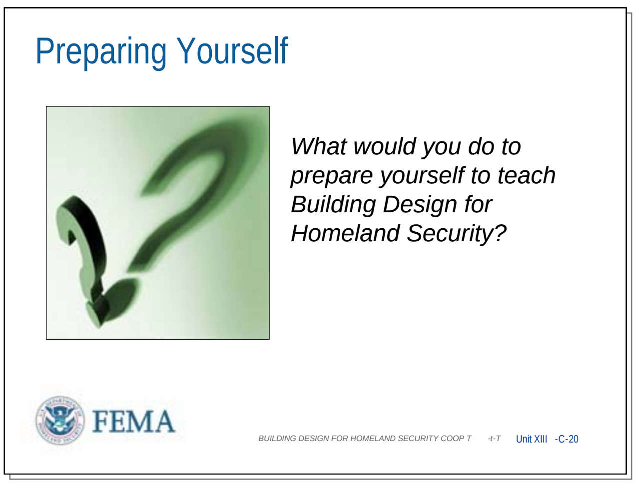
- FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, one per instructor and one per participant
- PowerPoint visuals (loaded on computer and backup CD)
- Student Reference CD, one per instructor and one per participant

Supplies

- Easel with paper pad refill, one per participant activity team
- Highlighter, one per participant
- Markers for use with easel pad, one package of various colors
- Name plate, one per instructor and participant
- Pen or pencil, one per participant
- Post-It® notes, smallest size available, one pad per participant
- Risk Matrix poster, one per table group
- Tablet, one per participant
- White board markers for use by participants to record case study activities information on the Risk Matrix poster, one per table group
- White board markers for use with slide acetates, as required if an Elmo projector is not available, one package of various colors

Training Site

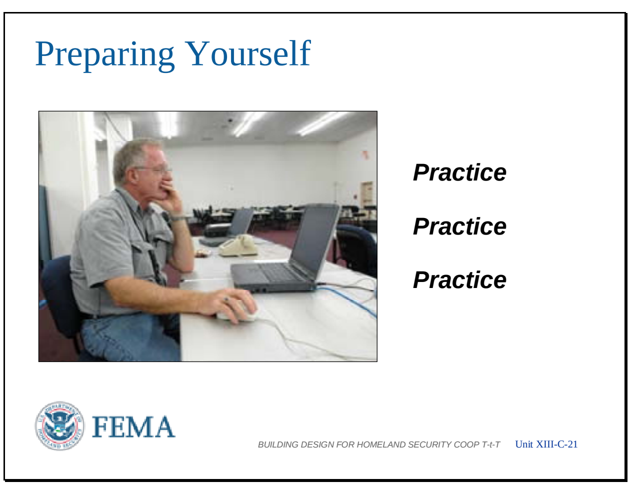
- Check all boxes of materials to ensure no surprises.
- Make sure the room is set up in table groups.
- Load the visuals on the desktop.
- Find out how to control the temperature and lights.



Preparing Yourself

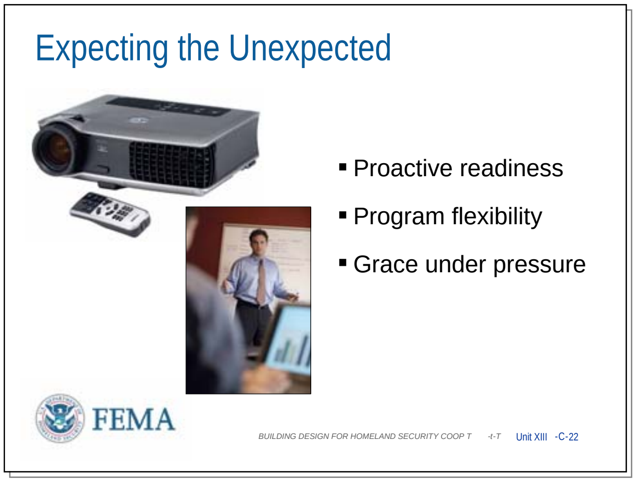
What would you do to prepare yourself to teach Building Design for Homeland Security?

- Review agenda
- Plan transitions
- Walk through course materials
- Accept nervousness as an energizer



Expecting the Unexpected

TIME: 12 Minutes



Ask participants what questions they have before you conclude the unit.

Expecting the Unexpected

What Could Happen?

This page intentionally left blank

Preparing To Train Adults

Instructional Skills

Prepared for:

Federal Emergency Management Agency
Emergency Management Institute

Revised January 2007

Contents

General Information

Purpose

The purpose of this reading packet is to teach you how to apply adult learning principles when instructing courses. It takes into consideration the unique characteristics including the learning styles and cultural backgrounds of your participants. As an instructor, you have probably asked yourself some or all of the following questions about adult learners:

- Can participants learn equally well?
- What motivates participants to learn?
- How do I know when learning has occurred?
- What instructional methods can I use to help participants learn the best?
- How can I accommodate the different learning styles and preferences of the participants when instructing?

The reading materials will address these questions. You will read about adult learning characteristics, adult learning principles, and learning styles and preferences. You will have several opportunities to practice applying the information presented by completing a series of practical exercises.

Objectives

After reading this packet, you will be able to:

- Discuss key adult learning characteristics.
- Explain the differences between training and learning.
- Use the principles of adult learning when instructing.
- Identify your own learning style.
- Accommodate different learning preferences when instructing.

Contents

How Adults Learn provides a basis for understanding adult learning by describing the physical, emotional, and intellectual characteristics of adult learners.

Adult Learning: Strategies for Success explains how to design and deliver effective training by following adult learning principles. These principles address the different physical, emotional, and intellectual characteristics that affect how adults learn.

Learners as Individuals summarizes the different learning preferences of adult learners and provides guidelines for accommodating learning preferences during training. While reading this section, you will complete the Learning Preferences Inventory that allows you to identify your own unique learning style.

How Adults Learn

Overview

Adults differ in interests, intelligence, life experiences, ability to concentrate, ability to remember, imagination, and sense of well being and self-confidence. Each of these factors influences how well and how fast a person learns and what you, as an instructor, must do to train adults effectively. This section provides a basis for understanding adult learning by describing the unique physical, emotional, and intellectual characteristics of adult learners. It also presents the differences between training and learning, and it prepares you for identifying when successful learning has occurred.

Highlights

When you complete this section, you will be able to:

- Describe the characteristics of adult learners.
- Explain the differences between training and learning.

Contents

Exercise:
Self-Assessment of Adult Learning

Instructions: This short exercise will help you assess your current understanding of adult learning.

True or False:

• Adults can learn equally well at every age throughout their lifespan.	☐ True	☐ False
• The greatest amount of vision loss in adults occurs after the age of 60 years.	☐ True	☐ False
• All adults experience a decline in their physical and sensory abilities as they grow older.	☐ True	☐ False
• Learning is an internal process that one's physical, emotional, and intellectual framework will affect.	☐ True	☐ False
• Adults engage in learning because they believe that it will help them cope with problems in later life. Their time perspective is one of postponed application.	☐ True	☐ False
• Adults benefit little from individualized attention and reinforcement.	☐ True	☐ False
• Studies have shown that most adults have a higher level of retention in learning when they read information rather than hear information.	☐ True	☐ False
• Adults rely heavily on the vicarious experiences of their instructors and textbooks.	☐ True	☐ False
• Most adults have preferred methods for learning new knowledge and skills.	☐ True	☐ False
• Adults learn best when the learning environment is informal and unstructured.	☐ True	☐ False
• Adults respond well to traditional, lecture-format learning.	☐ True	☐ False
• Like children, adults progress through developmental stages that impact their readiness to learn.	☐ True	☐ False

Answer Key:* *T, F, T, T, F, F, F, F, T, T, F, T

Adult Learning Characteristics

Social science and practical experience tell us that the characteristics of adult learners fall into three distinct categories:

- Physical characteristics
- Emotional characteristics
- Intellectual characteristics

Let's examine the physical characteristics of adult learners first. Physical traits such as lifelong learning abilities and physiological changes due to aging directly impact an adult's learning experiences.

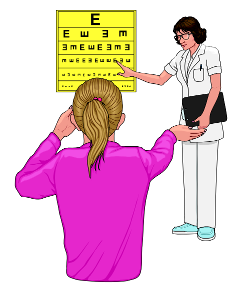
Physical Characteristics

Lifelong Learning

Unfortunately, many people still believe "you can't teach an old dog new tricks." This old adage is simply *not* true. Adults can learn throughout their lifespan, but they show a decline in the **rate** of learning with age. However, this decrease in the speed of learning occurs primarily in adults who get out of the practice of learning. Those who stay in practice can learn most things as well at 60 years of age as they could at 20, and they learn some things better.

Physiological Changes

Although adults can learn throughout their lifetime, they do experience a decline in their physical and sensory abilities as they grow older. Sometimes this affects their learning.



For example, all adults experience:

- **Vision Loss.** Beyond the age of 20 years, every person shows some decline in visual acuity. The greatest amount of vision loss occurs between the ages of 40 and 55 years.
- **Hearing Loss.** People reach their peak hearing performance before age 15, and then there is a consistent decline until age 65. Hearing loss in adults can have a marked influence on their level of self-confidence and can increase feelings of isolation.
- **Less Tolerance of Cold and Heat.** Adults show a lower tolerance for learning environments that are too warm or too cold.
- **Fatigue.** As adults get older, they tire more easily.

Not all physiological changes in adults are in the direction of decline. For example, although muscular strength, vigor, and speed of reaction tend to decline with age, other skills such as skill reliability and accuracy improve with practice.

In addition to the physical characteristics of adults that affect learning, there are emotional traits as well that help determine the success of adult learning experiences.

Emotional Characteristics

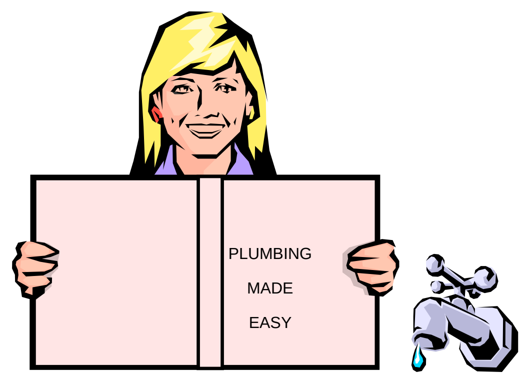
Independent Self-Concept

Adults see themselves as responsible, self-directing, and independent, and they want others to see them the same way. Adult learners tend to avoid, resist, and resent placement in situations where they are not treated like adults (e.g., being told what to do and what not to do, talked down to, embarrassed, punished, judged).

Often, adults fail to learn under conditions that are inconsistent with their feelings, thoughts, or actions.

Self-Motivated

In addition to having an independent self-concept, adults are also self-motivating. That is, adults *want* to learn when they have a *need* to do so. They want to know how the skill and/or knowledge will help them. Studies show that adults prepare themselves to learn by determining the benefits of learning, as well as the disadvantages of not learning.



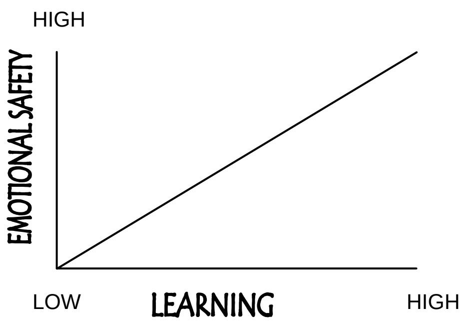
Reinforcement

Although adult learners are self-directed, they do benefit from, and respond positively to, reinforcement from their instructors and peers.

Established Emotional Frameworks

Another unique characteristic of adult learners is that they have established emotional frameworks that are part of their values, attitudes, and tendencies. Adult learning involves changing behaviors and possibly changing parts of this emotional framework. Change can be disorienting and anxiety provoking.

An adult's ability to change, and therefore to learn, is directly proportional to the degree of emotional safety he or she feels.



Immediate Application

Adults tell children that most of their learning will become useful to them in later life. Therefore, their time perspective of learning is one of postponed application. Adults, on the other hand, engage in learning largely in response to current life problems, pressures, and needs.

They believe that learning will improve their ability to deal with issues they face now. Hence, their time perspective of learning is one of *immediate* application.

Finally, with physical and emotional characteristics, there also are intellectual traits that directly influence learning in adults.

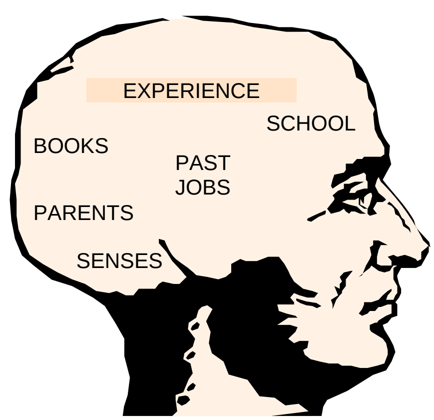
Intellectual Characteristics

Accumulated Experience

Adults enter educational activities with more life experiences than children. Having lived longer, adults have accumulated a much greater volume of experiences from which to draw. Adults also have different kinds of experiences than children. Adults, therefore, are a rich resource for one another's learning. They enjoy sharing experiences with other learners, and they tend to be less dependent on their instructors and textbooks.

Previous Learning

In addition to having a greater amount of accumulated experience than children, adult learners also possess a large bank of previous learning that can be both an asset and a liability. Previous learning can be beneficial because adults learn best when they are able to link new knowledge and skills with what they have learned previously. The linkage allows the adult learners to draw upon existing knowledge and skills and decreases anxiety about learning new areas.



Previous learning, however, can also be a hindrance to learning. If the new knowledge and skills to be acquired contradict the learner's existing knowledge and skills, then the learner:

- May dismiss or reject the new knowledge and skills and stick with what he or she knows and can do.
- May experience interference from the existing knowledge and skills as he or she tries to learn the new knowledge and skills. In this case, the adult learner needs to "unlearn" previous learning before acquiring the new knowledge or skill.

Active Learning

Another intellectual trait of adults that impacts learning is their need to participate actively in the instructional process. Adults learn by reading, listening, and watching, but they learn better when they are active participants in the learning process.

Studies show that 3 days after learning new information, adults retain[1]:

10% of What They Read 

20% of What They Hear 

30% of What They See 

50% of What They See and Hear 

70% of What They Say 

90% of What They Say as They Do It

Studies also show that adults have unique learning preferences, as the next section describes.

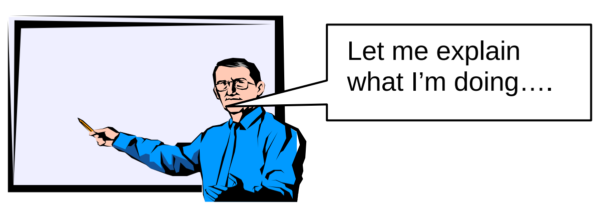
Learning Preferences

Most adults have preferred methods for learning new knowledge and skills. Adult learners respond better when the presentation of new material utilizes a variety of instructional methods. This appeals to their different senses.

The section that begins on page 20 covers learning preferences in detail.

Adult learners respond better when the new material utilizes a variety of instructional methods.

[1] Sharon Fisher, *Adult Learning*, Amherst, MA: Human Resource Development Press, Inc., 1988.



Training is Different from Learning

Too often, educators and trainers make the mistake of believing that successful learning has occurred simply because they have communicated certain information or demonstrated skills to their participants. Training, however, does not always result in learning. There are specific criteria you can use to determine whether learning has actually occurred.

Training Versus Learning

The term *training* applies to any manner of imparting information or skills that others may learn. In comparison, *learning* is the acquisition and mastery of such knowledge or skills. In other words, learning is an end product of successful training.

As an instructor, it is your job to eliminate barriers to learning so that learning will be observable, applicable, and verifiable.

Training ≠ Learning

Training does not always result in learning for many reasons, including:

- During training, learners can become inattentive, thus failing to acquire and master the knowledge and skills necessary for learning.
- The instructor's style and techniques do not match the learners' preferences.
- The knowledge and skills being taught may be too complex for the audience, who may become bored, confused, or frustrated.
- The learners see no direct value in learning the material.
- Training may be all theory and no practice.

Learning is an end product of successful training.

To prove that learning has occurred, you should use the following criteria:

- There is an **observable** change in behavior. Both the learner and the instructor observe a change in behavior.
- The learner applies the knowledge and skills in practice exercises.
- Valid and reliable testing verifies the acquisition and mastery of knowledge and skills.

(

As an instruc our job to
eliminate bar rning so that
learning will le,
applicable, a e.

LEARNING MUST BE:

☑ OBSERVABLE

☑ APPLICABLE

☑ VERIFIABLE

Exercise:
Has Learning Occurred?

Instructions: Read each of the following learning situations and determine whether or not learning has really taken place. Explain (in the appropriate space) how you know that learning has or has not occurred.

Learning Situation #1:

A group views a video about blast effects.

Has learning occurred? Yes _____ No _____

If yes, explain how you know learning has occurred. If no, explain how you know that learning has not occurred.

Learning Situation #2:

In training, Bill Baker encounters the Threat-Vulnerability Matrix for the first time. From the lecture he becomes familiar with the matrix, but in a practical exercise, he cannot determine the risk rating for each asset-threat/hazard pair.

Has learning occurred? Yes _____ No _____

If yes, explain how you know learning has occurred. If no, explain how you know that learning has not occurred.

Answer Key: #1-No, there was not an observable change in behavior because the learner did not practice applying the knowledge from the video. #2-No, the learner was unable to apply the new knowledge during a practical exercise.

Job Aid #1:
Adult Learning Characteristics

The following summarizes the characteristics of adult learners. Use this checklist as a guide when preparing training presentations.

- ☑ Adults, when older, may not be able to hear or see as well as they could when they were younger.
- ☑ Adults are less inclined to be impulsive; they require time to think through problems.
- ☑ Adults see themselves as capable of self-direction.
- ☑ Adults need to have a part in determining what they learn.
- ☑ Adults must want to learn before learning takes place.
- ☑ Adults have values, attitudes, and tendencies that influence their willingness to learn.
- ☑ Adults need individual attention and reinforcement to achieve personal goals.
- ☑ Adults possess a large volume of previous learning that influences learning.
- ☑ Adults learn by doing.
- ☑ Adults may not respond well to lectures.
- ☑ Adults must have training methods adapted to their needs.
- ☑ Adults prefer a variety of training methods.
- ☑ Adults learn best in an informal environment.
- ☑ Adults need to transfer new learning to their situations.
- ☑ Adults learn by sharing experiences.
- ☑ Adults stimulate each other.
- ☑ Adults want practical knowledge and skills.
- ☑ Adults prefer specific usable information rather than theoretical information.
- ☑ Adults have other responsibilities that may distract them or call them away from class.

Adult Learning: Strategies for Success

Overview

The unique adult learning characteristics you read about in the previous section point out the need for some specific strategies to use when designing and delivering training to adults. By following the strategies this section introduces, you will increase the likelihood of motivating adult participants and ensuring that learning occurs.

Highlights

When you complete this section, you will be able to use specific strategies effectively for addressing adult learning characteristics when training.

Contents

Exercise: How Adult Learning Characteristics Impact Training

Instructions: For training to be successful, you must understand how adult learning characteristics impact the way you plan and deliver your training. Review the adult learning characteristics in the left-hand column, and, for each characteristic, select the most appropriate training strategy from the right-hand column. When you finish this matching exercise, check your answers against the answer key on bottom of this page.

Adult Learning Characteristic

_____ Adults can learn by reading, listening, and watching, but they learn best if they participate actively in the learning process.

_____ Most adults have preferred methods for learning new knowledge and skills.

_____ Adults engage in learning in order to help them cope with current issues and problems. They seek learning that they can apply immediately.

_____ Adults have a large bank of previous learning that can be both an asset and a liability to learning.

_____ Adults enter training with a large volume of life experiences from which to draw.

_____ Adults perceive themselves as independent and capable of self-direction. They desire others to see them the same way.

_____ All adult learners experience a decline in sensory abilities (e.g., hearing, vision, physical conditioning).

Training Strategy

a. Plan your training so that you measure successful learning in terms of accuracy and reliability, rather than speed and volume.

b. Provide learners with opportunities to identify what they want and need to learn; to plan and to carry out their own learning activities; and to evaluate their own progress toward self-selected goals.

c. Plan training activities around your participants' issues and concerns about what they will be doing in their jobs.

d. Maximize learning by doing.

e. Provide job aids to assist in "unlearning" previous information that is interfering with new learning.

f. Match the instructional methods you select to your participants' learning preferences.

g. Use the learners' life experiences to introduce and discuss new concepts.

Answer Key: d, f, c, e, g, b, a

Training Strategies That Address Adult Learning Characteristics

There are many specific strategies you can use in training to address the physical, emotional, and intellectual factors of adult learning that was covered previously. Using these strategies will enable you to maximize the participants' learning by:

- Creating an environment that optimizes learning.
- Making the learning applicable to adults' past learning and present situation.
- Actively involving the learners in the training process.

Strategies to Address Physical Characteristics

Lifelong Learning

To help adults learn well at any age, you should create a learning environment that meets the needs and abilities of your adult learners. Creating this environment involves:

- Developing your activities so that you measure successful learning in terms of accuracy and reliability rather than speed and volume.
- Providing learning exercises that require analysis and processing rather than impulsive, "quick-on-your-feet" responses.

The Reality

We realize that learning conditions may be less than perfect when you are teaching. Recognizing the importance of the physical environment will allow you to do as much as is within your control, given your particular conditions.

Physiological Changes

The following techniques will provide a learning environment that minimizes the extent to which learners' physical conditioning and health interfere with learning:

- Provide good lighting without glare.
- Provide sound amplification with good acoustics.
- Provide conditions that minimize fatigue and anxiety.
- Allow adult learners to take breaks.
- Provide healthful food during breaks.
- Use job aids and memory-enhancement devices to help learners retain information.

Strategies to Address Emotional Characteristics

Independent Self-Concept

In order to respect adults' independent self-concepts, you need to provide your learners with opportunities to identify what they want and need to learn; to plan and to carry out their own learning activities; and to evaluate their own progress toward self-selected goals.

Follow these strategies to accomplish this objective:

- Assume the role of "learning resource" rather than the more traditional role of teacher.
- Allow adult learners to direct their own learning as much as possible.
- Treat adult learners as adults. Avoid "talking down" to adult learners. Instead, use content and style appropriate to their developmental level.
- Avoid putting adult learners in situations where they will feel embarrassed.

MY GOALS:

I need to learn…

I want to learn…

Reinforcement

Adults respond positively to reinforcement. So, as an instructor, you should:

- Respond to the verbal and nonverbal feelings that adult learners express.
- Provide meaningful reinforcement to adult learners. Learners must perceive the reinforcement as positive from their frames of reference.
- Provide opportunities for peer feedback and reinforcement. Reinforcement from other adult learners can be as powerful as the reinforcement that instructors provide.

Self-Motivated

Adults are self-motivated learners. Follow these strategies to address this adult learning characteristic:

- Make sure that adult learners get an opportunity to explore why they need to learn the knowledge or skills the training will present.
- Make learning activities relevant to the participants' learning objectives.
- Explain the possible benefits to gain by learning the knowledge or skills to be presented.
- Provide opportunities to apply and try out new learning as part of training. Instructors can motivate adult learners by convincing them of benefits. However, to stay motivated, adult learners need a chance to see the benefits for themselves.

Established Emotional Frameworks

Because adult learners have established values, attitudes, and tendencies, and because learning involves changing parts of this framework, you should:

- Provide a learning environment that is non-threatening.
- Avoid making adult learners change too many behaviors all at once. Have them learn one new behavior and master it before attempting to learn another new behavior.
- Allow adult learners to hang on to established values, attitudes, and tendencies, **unless** these get in the way of learning.

Immediate Time Perspective

Adults engage in learning largely in response to current life problems, pressures, and needs. Therefore, you should:

- Plan your training activities around your learners' issues and concerns.
- Make the training problem-centered, not subject matter-centered.
- Emphasize your function as one of helping learners look at problems and try new approaches.
- Don't tell your learners what would be "good for them."

Strategies to Address Intellectual Characteristics

Accumulated Experience

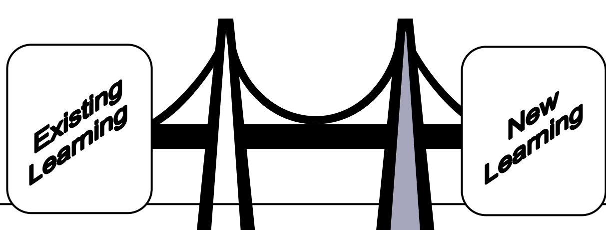
To draw upon the adults' extensive life experiences, you should:

- Use instructional techniques that tap the learners' experience, such as group discussion, case studies, role playing, demonstrations, group interviews, and skill practice exercises.
- Use your learners' life experiences to introduce and discuss new concepts.

Previous Learning

Help your learners build bridges between existing learning and new learning by:

- Using analogies and common examples when instructing.
- Allowing learners to explore what they know about an area before providing instruction.
- Giving learners credit for what they know or are able to do.
- Using learners who have mastered areas to assist other learners.
- Providing job aids or helping learners develop their own job aids to assist in "unlearning" previous learning that is interfering with new learning.



Active Learning

Involve your adult learners in the learning process. Some suggested strategies are:

- Pair lectures or reading assignments with activities such as discussions, exercises, practice activities, role plays, and job simulations.
- Maximize "learning by doing."

Exercise:

Applying Training Strategies to Past Experiences

The purpose of this exercise is to help you validate the training strategies that this section just discussed by applying them to your own past experiences as an adult learner. Follow the instructions below to complete this exercise.

1. Think of one training session you attended in the past that was **ineffective** for you as an adult learner. Jot down the ineffective elements in the appropriate space below. Write the strategies that were used during the training across from each element.

INEFFECTIVE TRAINING

Ineffective Elements	Strategies Ignored

2. Think of one training session you attended in the past that was **effective** for you as an adult learner. Jot down the effective elements in the appropriate space below. Write the strategies that were used during the training across from each element.

EFFECTIVE TRAINING

Effective Elements	Strategies Used

Instructor Effectiveness Inventory

Instructions: Evaluate yourself as an instructor by answering the following questions in preparation for an effective training session. Answering "no" to any of these questions indicates a need to adjust your training strategy to meet the needs of your learners. **If you have never instructed, just read this job aid; do not check the boxes.**

DO YOU AS AN INSTRUCTOR:	***YES***	***NO***
Provide a learning environment that minimizes the extent to which the learners' physical conditioning and health interfere with learning?	☐	☐
Provide breaks for learners?	☐	☐
Use job aids and other memory-enhancement devices?	☐	☐
Allow your learners to identify what they want and need to learn?	☐	☐
Allow your learners to set their own goals?	☐	☐
Relate the material to the learners' goals?	☐	☐
Treat learners like adults?	☐	☐
Focus on "real world" problems?	☐	☐
Repeatedly reinforce skills and knowledge through various learning methods and participant practice?	☐	☐
Provide a learning environment that is non-threatening?	☐	☐
Provide meaningful reinforcement to learners?	☐	☐
Provide learning activities that relate to the learners' experience?	☐	☐
Involve participants in the learning process and minimize passive learning?	☐	☐
Allow for useful debate and exchange of ideas?	☐	☐
Identify and accommodate for participants' learning preferences?	☐	☐
Use a variety of instructional methods?	☐	☐
Inform your learners of what you expect of them at the end of training?	☐	☐

Learners as Individuals

Overview

Each time you lead a training course, you will face the different learning styles and preferences of your participants. Some participants may learn better through visual stimulation, while others may better acquire knowledge through auditory means. Some participants may prefer to learn with background sound, such as classical music, while others need complete silence to concentrate. Some participants will prefer to study with others, while some may be more productive working on their own. This section will prepare you to identify your learners' preferences and will take steps to accommodate their different learning styles.

Highlights

When you complete this section, you will be able to:

- Identify your own learning style.
- Identify others' learning preferences and strategize ways to accommodate them when instructing.

Contents

Learning Styles and Preferences

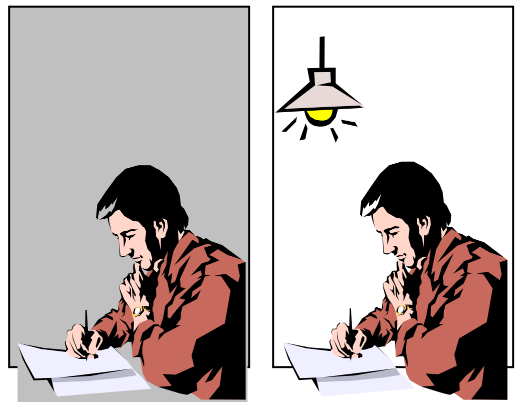
Most adults have preferred methods for learning new knowledge and skills. Adult learners respond better when an instructor presents new material through a variety of instructional methods. This appeals to their different senses. Adult learners may have preferences about any or all of the following factors.

Physical Factors

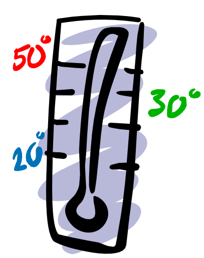
Learners have different preferences regarding their physical environment, including:

- ***Noise Level:*** Some learners can block out surrounding noises and function effectively despite noisy distractions. Other learners can adjust only to selected sounds and require that nearly all noisy distractions be eliminated. Still others prefer specific background sounds while studying.

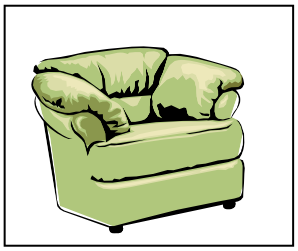
- ***Lighting:*** Room illumination also appears to affect the learning process. Some learners can function with ease only when the learning setting is well lit. However, other learners may consider that same degree of lighting to be excessive. If the lighting is incorrect for the learner, it can reduce concentration by over stimulating the learner or by lulling the learner to sleep.



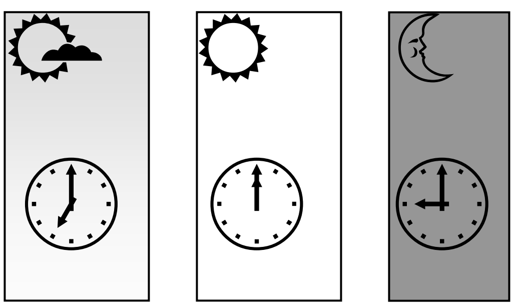
- ***Room Temperature:*** Room temperature is another environmental factor that can affect one's ability to learn. Some learners require a warm environment before they can study, while other learners may find the amount of warmth that relaxes certain learners actually makes them uncomfortable. Some learners function best in a cool room, while other learners are not at their best unless they are in a warm setting.



- ***Room Setting:*** The structure of the room setting can also affect one's ability to learn. Some learners prefer an informal setting such as a lounge area or their own living room. Other learners concentrate best when they are studying at a desk in a more formal setting.



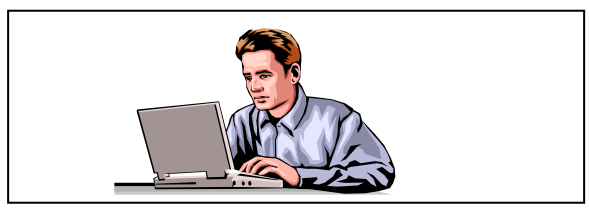
- ***Time of Day:*** The final preference area in the physical dimension is the time of day. Each of us develops our own internal clock, making us more alert at certain times of the day. Therefore, some learners concentrate and learn best in the morning. Other learners are most productive in the afternoon or evening.



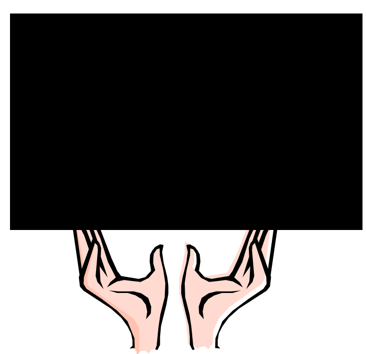
Besides having preferences about their physical learning environment, adults also have a variety of emotional needs that impact their ability to learn.

Emotional Factors

- ***Social Needs:*** Individuals have different social needs when learning. Learning can occur when learners work alone, with someone else, or with a small group. The learning task may influence this preference. For example, your learners may prefer to work alone when learning theoretical material, but prefer to work with someone else when applying the theory to a real problem. Even though your learners will probably engage in learning both alone and with others, they may prefer one arrangement over the other.



- ***Motivation:*** In addition to having different social preferences, adults also have unique motivational needs. Motivation is a necessary ingredient for learning.



Extrinsic motivation may come from external sources such as clients and fellow employees. Motivation can also be intrinsic, or in other words, come from inside ourselves. Learners usually need a combination of extrinsic and intrinsic motivation. However, individual learners may have a strong preference for one source of motivation above the other.

When motivation is extrinsic, we depend on receiving external reinforcement. External reinforcement may include anything we like or want. The same external reinforcement may not work for everyone.

Intrinsic motivation is another way of saying self-motivation. When we are intrinsically motivated, we are not looking for some external source of reinforcement. Rather, we are reinforcing ourselves. An example of internal reinforcement is feeling good about one's self after mastering a new skill: "I conducted that training course even more smoothly than the last one!"

Adults also differ in intellectual factors known as learning styles, which describe how they acquire and retain information. Some adults learn best by *hearing* information, others by *seeing* information, and still others by *touching* and *doing*.

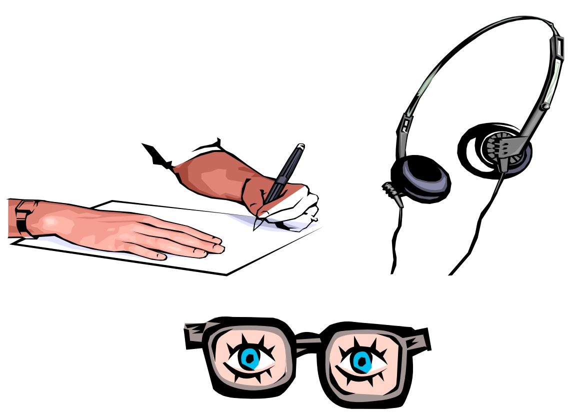
Intellectual Factors

Adults have different learning styles, including:

- ***Auditory:*** Some adults may be auditory learners. Auditory learners are those who can easily differentiate among sounds and can reproduce symbols, letters, or words by hearing them. Learners who favor auditory learning must be able to remember what they just heard.

Some adults learn best by hearing information, others by seeing information, and still others by touching and doing.

While auditory learning can enhance learning for some people, it can also frustrate learning for others. Some learners prefer to read words rather than hear them spoken. Reading allows the learner to set the pace and review passages with ease.



- ***Visual:*** Adults can also be visual learners who learn best by seeing an image or conjuring up an image in their mind. These learners prefer instructional materials that include many maps, pictures, symbols, graphs, and lists.

- ***Kinesthetic:*** Finally, adults who are kinesthetic learners learn best through their tactile sense or through experience—in other words, by touching or doing. For example, kinesthetic learners find it easier to remember things that they have written down over things that they have heard. A kinesthetic learner is the one who underlines in bold or takes notes while reading.

All learning is ultimately kinesthetic. Learners' preferences relate to the timing of the kinesthetic experience and the amount of kinesthetic experiences needed. Strong kinesthetic learners need practice exercises early in the learning process.

Other learners prefer to engage in kinesthetic experiences only after they have mastered new learning through auditory or visual means.

All learning is ultimately kinesthetic.

As instructors, you must be able to identify the unique learning styles and preferences of your participants and accommodate these differences with a variety of instructional techniques, methods, and media. The following job aid summarizes individual learning styles and suggests strategies for accommodating your learners' styles.

Job Aid #2:

Accommodating Individual Learners

This table summarizes individual learning preferences and provides strategies for accommodating your learners' unique learning styles, whenever it is possible to do so.

IF YOUR LEARNERS PREFER:	***THEN:***
PHYSICAL FACTORS • Background noise while studying	• Play soft music during your instruction. • Encourage your learners to study in open places like lounges, rather than quiet libraries.
• A quiet learning setting	• Encourage your learners to use ear plugs or a special audiotape with "white noise" when studying. (White noise is nonspecific noise that can block out other noise.) • Arrange for periods of quiet time.
• A brightly lit learning setting	• Select learning environments with a lot of windows or other sources of direct light.
• A darker learning setting	• Select darker learning environments without a lot of windows or direct light. • Encourage these learners to move away from the windows and other sources of direct light. • Encourage these learners to wear tinted glasses to cut down on the amount of light or glare.
• A warm learning climate	• Encourage learners to sit near the heating source and bring extra clothing.

Job Aid #2:
Accommodating Individual Learners
(Continued)

IF YOUR LEARNERS PREFER:	***THEN:***
PHYSICAL FACTORS *(Continued)*	
• A cool learning climate	• Encourage learners to move away from the heating source and wear cool clothing. • Adjust the room temperature by opening windows, lowering the thermostat setting, or bringing in fans.
• Studying in the morning	• Arrange your lesson plans so that: - You cover the more difficult areas in the morning when learners have the most energy. - Learners work on the easiest areas in the afternoon.
• Studying in the afternoon	• Arrange your lesson plans so that: - Learners work on the easiest areas in the morning. - You save the more difficult areas for the afternoon when learners have the most energy.
EMOTIONAL FACTORS	
• Learning alone	• Prepare a lot of individualized learning activities for your group.

Job Aid #2:
Accommodating Individual Learners
(Continued)

IF YOUR LEARNERS PREFER:	*THEN:*
EMOTIONAL FACTORS *(Continued)* • Learning with others	• Prepare a lot of group activities for your learners.
• Extrinsic motivation	• Provide a lot of individualized attention and positive reinforcement to your learners. • Have peers provide feedback to one another.
• Intrinsic motivation	• Continue to provide reinforcement, but to a lesser degree than with extrinsically motivated learners.
INTELLECTUAL FACTORS • Auditory learning	• Encourage learners to talk through steps in an activity. • Encourage oral reporting. • Use tape-recorded instruction and other audio equipment.
• Visual learning	• Provide visual directions and demonstrations. • Use maps, graphs, charts, and other visual aids.
• Kinesthetic learning	• Encourage your learners to take notes while they read, listen, or watch. • Employ role-playing and simulation exercises. • Let learners assist you in creating learning aids.

Learning Preference Inventory

Instructions: Read each statement below. Indicate your level of disagreement or agreement with each statement by circling a number to the right of the statement.

	Strongly Disagree 1	Disagree 2	Neither Disagree Nor Agree 3	Agree 4	Strongly Agree 5
1. When I read, I like to have a lot of light.	1	2	3	4	5
2. I learn well by hearing how to do something; i.e., from a tape, a record, or a lecture.	1	2	3	4	5
3. I would rather study in a library than in a lounge.	1	2	3	4	5
4. I find it difficult to study when there is music in the background.	1	2	3	4	5
5. I feel that I am self-motivated.	1	2	3	4	5
6. I work or study well in the evening.	1	2	3	4	5
7. I have trouble concentrating when I am working or studying with other people.	1	2	3	4	5
8. I like to draw or use diagrams when I learn.	1	2	3	4	5

Learning Preference Inventory (Continued)

	Strongly Disagree 1	Disagree 2	Neither Disagree Nor Agree 3	Agree 4	Strongly Agree 5
9. I am comfortable at times when those around me say it's too warm.	1	2	3	4	5
10. I like my family or friends to know that I do a good job at work.	1	2	3	4	5
11. I enjoy learning new things about my work.	1	2	3	4	5
12. It's difficult for me to concentrate when I am cold.	1	2	3	4	5
13. Noise and background conversations and/or music really bother me when I have to concentrate.	1	2	3	4	5
14. I work or study well in the afternoon.	1	2	3	4	5
15. I prefer to work or study alone.	1	2	3	4	5
16. I have trouble studying when I sit on a soft chair or couch or lie on the floor.	1	2	3	4	5
17. When I work, I like to turn on all the lights.	1	2	3	4	5
18. I like my instructors or supervisors to recognize my efforts.	1	2	3	4	5
19. I learn well by trying to do things myself, with my own hands.	1	2	3	4	5

Learning Preference Inventory (Continued)

	Strongly Disagree 1	Disagree 2	Neither Disagree Nor Agree 3	Agree 4	Strongly Agree 5
20. I concentrate best when I am sitting up at a desk.	1	2	3	4	5
21. I would rather be warm than cold.	1	2	3	4	5
22. I prefer working in bright light.	1	2	3	4	5
23. The things that I remember best are the things that I hear.	1	2	3	4	5
24. I learn best by *doing* on the job.	1	2	3	4	5
25. I get a lot of satisfaction from doing the best I can.	1	2	3	4	5
26. I work better when I know that my work will be checked.	1	2	3	4	5
27. I learn well by seeing how to do something; i.e., looking at a diagram or picture, or watching someone else do it.	1	2	3	4	5
28. I get less done when I work with someone else.	1	2	3	4	5
29. I work or study well in the morning.	1	2	3	4	5
30. I find it difficult to block out noise when I am trying to work.	1	2	3	4	5

Scoring Your Learning Preference Inventory

Instructions: Take your scores from the Learning Preference Inventory and enter each item score where indicated on this score sheet. Add the item scores under each category to get an idea of your learning preferences.

Physical Preferences: Learning Setting

Noise Level	Item #	Score
	4	_____
	13	_____
	30	_____
	Total Score	_____

- Total scores of **10 or more** indicate that noises bother you when you are trying to learn.
- Total scores of **9 or less** indicate that noises do *not* bother you when you are trying to learn

Lighting	Item #	Score
	1	_____
	17	_____
	22	_____
	Total Score	_____

- Total scores of **10 or more** indicate that you prefer to learn in bright lighting.
- Total scores of **9 or less** indicate that you do *not* prefer to learn in bright lighting.

Physical Preferences: Learning Setting (Continued)

Temperature	Item #	Score
	9	______
	12	______
	21	______
	Total Score	______

- Total scores of **10 or more** indicate that you prefer to learn in warmer temperatures.
- Total scores of **9 or less** indicate that you prefer to learn in cooler temperatures.

Structure	Item #	Score
	3	______
	16	______
	20	______
	Total Score	______

- Total scores of **10 or more** indicate that you prefer a **formal** learning setting.
- Total scores of **9 or less** indicate that you prefer an **informal** learning setting.

Physical Preferences: Time of Day

	Item #	Score
Morning Score	29	_____
Afternoon Score	14	_____
Evening Score	6	_____
	Total Score	_____

- Total scores of **4 or 5** indicate a preference for learning at that time of day.
- You may have more than one time preference for learning, or time may not make a difference to you.

Emotional Preferences: Social Needs

Alone or With Others	Item #	Score
	7	_____
	15	_____
	28	_____
	Total Score	_____

- Total scores of **10 or more** indicate that you prefer to learn alone.
- Total scores of **9 or less** indicate that you prefer to learn with other people.

Emotional Preferences: Motivation

Extrinsic Motivation	Item #	Score
	10	_____
	18	_____
	26	_____
	Total Score	_____

- Total scores of **10 or more** indicate that external reinforcements may be important to you.
- Total scores of **9 or less** indicate that external reinforcements may *not* be very important to you.

Intrinsic Motivation	Item #	Score
	5	_____
	11	_____
	25	_____
	Total Score	_____

- Total scores of **10 or more** indicate that you seem to be self-motivated.
- Total scores of **9 or less** indicate that you may *not* be self-motivated.

Intellectual Preferences: Learning Styles

Auditory Learning	Item #	Score
	2	_____
	23	_____
	Auditory Total	_____

Visual Learning	Item #	Score
	8	_____
	27	_____
	Visual Total	_____

Kinesthetic Learning	Item #	Score
	19	_____
	24	_____
	Kinesthetic Total	_____

- In each area (auditory, visual, kinesthetic), total scores of 7 or more indicate a preference for that type of learning.
- You may prefer more than one type of learning, or types of learning may not make a difference to you.

Job Aid #3: Strategies for Addressing Insensitive Events

Listed below are examples of events that may occur during training that add to personal biases and stereotypes and that fail to show respect for differences in people. Also included are possible strategies for responding appropriately to these events in the training room. It is critical that, as an instructor, you are aware of these events and that you are prepared to respond appropriately. Refer to this when preparing for training.

POSSIBLE EVENT	***STRATEGY***
Telling jokes about gender, ethnicity, or a profession.	• Do *not* publicly denounce the person telling the joke. • As soon as the person has finished telling the joke, announce that these types of jokes are inappropriate and illegal and will not be tolerated.
Praising or negatively reinforcing only some participants.	• Be aware of your own biases, and concentrate on recognizing *all* participants equally. • Avoid negative reinforcement (e.g., punishing, sarcasm, putting down participants) altogether.
Failing to prepare for a participant with special needs.	• Apologize to the participant. • Ask the participant how you can be of assistance. • In the future, be aware of who your course participants are so you can prepare for those with special needs.
Making sexual remarks.	• Inform the offender(s) that making sexual remarks is illegal and will not be tolerated in the training room. • If a participant has been offended by the remarks, ask the offender to apologize.

Reading Assessment

Instructions: Place your answers to the following questions on the answer sheet on page 40. When you finish this assessment, check your answers against the answer key on page 42.

1. Which of the following combinations of training methods is **most** consistent with adult learning principles?

   a. Lectures and reading assignments
   b. Reading assignments, demonstrations, and tests
   c. Reading assignments, group discussions, and practical exercises
   d. Lectures and case studies

In questions 2 through 5, match the descriptions on the left with the correct learning style on the right.

2. I get a lot of satisfaction from doing the best I can.
3. I learn well by seeing how to do something.
4. I work better when I know my work will be checked.
5. I learn well from videos and lectures.

a. Visual Learning
b. External reinforcement
c. Internal reinforcement
d. Social needs
e. Auditory learning

6. John has felt unprepared in responding to questions from COOP facility managers about their mitigation options. In response, he has searched DOD and DHS websites for best practices. Which adult learning characteristic is being illustrated in this scenario?

   a. Active learning. Adults learn best when they are active participants in the learning process.
   b. Immediate application. Adults engage in learning to help them deal with issues they face now.
   c. Accumulated experience. Adults bring more life experiences to the learning environment than children.
   d. Reinforcement. Adult learners benefit from, and respond to, reinforcement.

1. Reading Assessment (cont'd)

7. Tom is conducting *Building Design for Homeland Security*. During his workshop, a participant cracks a joke about a particular ethnic group. What is the most appropriate way for Tom to handle this event?

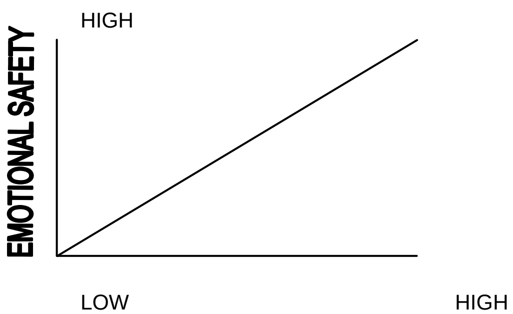
   a. At the next break, take the person aside and tell him or her that these types of jokes are inappropriate and illegal.

   b. As soon as the person has finished telling the joke, announce that these types of jokes are inappropriate and illegal and will not be tolerated.

   c. Laugh now, but tell the person about your discomfort later in private.

   d. Use the situation as an opportunity to discuss cultural sensitivity with the entire class.

8. With the Y axis labeled Emotional Safety, what should the X axis be labeled?



   a. Practice

   b. Number of instructors

   c. Learning

   d. Number of course participants

9. Select the method from which adults will retain the most information after 3 days.

   a. Information they speak
   b. Information they hear
   c. Information they read
   d. Information they see

10. You involve your participants in the learning process by combining reading assignments with job simulations. This is an example of which adult intellectual characteristic?

   a. Accumulated experience
   b. Active learning
   c. Previous learning
   d. Physiological changes

11. One can learn more effectively by:

   a. Engaging in the class and in small group activities.
   b. Listening to lecture and taking notes.
   c. Working alone and asking the presenter questions.
   d. Expecting to be entertained during training.

12. During the morning session, you notice that course participants seem very tired. After lunch, you decide to address the fact that they have a low energy level. What learning activity should you select?

   a. Video
   b. Lecture
   c. Group exercise
   d. Power Point presentation

3. Reading Assessment (cont'd)

13. A participant who draws diagrams and pictures to understand information, and who learns new skills best by watching others, is most likely a:

    a. Visual learner
    b. Auditory learner
    c. Social learner
    d. Self motivated learner

For questions 15 through 20, review the adult learning characteristic on the left and determine the most appropriate training strategy from the right.

14. Adults can learn by reading, listening, and watching, but they learn best if they participate actively in the learning process.

15. Most adults have preferred methods for learning new knowledge and skills.

16. Adults engage in learning in order to help them cope with current issues and problems. They seek learning that they can apply immediately.

17. Adults have a large bank of previous learning that can be both an asset and a liability to learning.

18. Adults enter training with a large volume of life experiences from which to draw.

19. Adults perceive themselves as independent and capable of self-direction. They desire others to see them in the same way.

a. Provide learners with opportunities to identify what they want and need to learn; to plan and to carry out their own learning activities; and to evaluate their own progress toward self-selected goals.

b. Plan training activities around your participants' issues and concerns.

c. Maximize learning by doing.

d. Provide job aids to assist in "unlearning" previous information that is interfering with new learning.

e. Match the instructional methods you select to your participants' learning preferences.

f. Use the learners' life experiences to introduce and discuss new concepts.

Reading Assessment

ANSWER SHEET

1. ______
2. ______
3. ______
4. ______
5. ______
6. ______
7. ______
8. ______
9. ______
10. ______
11. ______
12. ______
13. ______
14. ______
15. ______
16. ______
17. ______
18. ______
19. ______

Reading Assessment

ANSWER KEY

1. c
2. c
3. a
4. b
5. e
6. b
7. b
8. c
9. a
10. b
11. a
12. c
13. a
14. c
15. e
16. b
17. d
18. f
19. a

Unit XIV (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer
UNIT TITLE	Course Wrap-Up
OBJECTIVES	1. Reflect upon the reasons for attending the course provided during Unit 1 Introductions (any Case Study version) and the conduct of course. a. Expectations met? b. Likes and dislikes? c. Value? 2. Provide written feedback to the Course Director and Instructors through course evaluation forms and verbal comments related to the course specifically or building design for Homeland Security in general. This feedback is critical to improving the course.
SCOPE	The following topics will be covered in this unit: 1. Discussion of general issues and concerns. 2. Course evaluations – forms and verbal comments. 3. Distribution of course certificates.
REFERENCES	No references are required for this unit.

This page intentionally left blank