Risk Management Series

Risk Assessment

A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings

FEMA 452 / January 2005

FEMA

Department of Veterans Affairs

FEMA 452 / *January 2005*

RISK MANAGEMENT SERIES

Risk Assessment
A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings

PROVIDING PROTECTION TO PEOPLE AND BUILDINGS

FEMA

www.fema.gov

with cooperation from the Department of Veterans Affairs

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

FOREWORD AND ACKNOWLEDGMENTS

BACKGROUND

The Federal Emergency Management Agency (FEMA) developed this Risk Assessment, A How-To Guide to *Mitigate Potential Terrorist Attacks Against Buildings,* to provide a clear, flexible, and comprehensive methodology to prepare a risk assessment. The intended audience includes the building sciences community of architects and engineers working for private institutions, building owners/operators/managers, and State and local government officials working in the building sciences community.

OBJECTIVE AND SCOPE

The objective of this How-To Guide is to outline methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. Based on those considerations, the methods presented in this How-To Guide provide a means to assess the risk to the assets and to make risk-based decisions on how to mitigate those risks. The scope of the methods includes reducing physical damage to structural and non-structural components of buildings and related infrastructure, and reducing resultant casualties during conventional bomb attacks, as well as chemical, biological, and radiological (CBR) agents. This document is written as a How-To Guide. It presents five steps and multiple tasks within each step that will lead you through a process for conducting a risk assessment and selecting mitigation options. It discusses what information is required to conduct a risk assessment, how and where to obtain it, and how to use it to calculate a risk score against each selected threat.

This is one of a series of publications that address security issues in high-population, private sector buildings. This document is a companion to the *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (FEMA 426) and the Building Design for Homeland Security Training Course (FEMA E155). This document also leverages information contained within the *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks (*FEMA 427).

The primary use of this risk assessment methodology is for buildings, although it could be adapted for other types of critical infrastructure.

The foundation of the risk assessment methodology presented in this document is based on the approach that was developed for the Department of Veterans Affairs (VA) through the National Institute for Building Sciences

(NIBS). Over 150 buildings have been successfully assessed using this technique. The risk assessment methodology presented in this publication has been refined by FEMA for this audience.

The purpose of this How-To Guide is to provide a methodology for risk assessment to the building sciences community working for private institutions. It is up to the decision-makers to decide which types of threats they wish to protect against and which mitigation options are feasible and cost-effective.

This How-To Guide views as critical that a team created to assess a particular building will be composed of professionals capable of evaluating different parts of the building. They should be senior individuals who have a breadth and depth of experience in the areas of civil, electrical, and mechanical engineering; architecture; site planning and security engineering; and how security and antiterrorism considerations affect site and building design.

The information contained in this document is:

- not mandatory
- not applicable to all buildings
- not applicable when it interferes with other hazards such as fire

ORGANIZATION AND CONTENT

In order to create a safe environment, many factors must be considered. Figure 1 depicts the risk assessment process presented in this document to help identify the best and most cost-effective terrorism mitigation measures for a building's own unique security needs. The first step is to conduct a threat assessment wherein the threat or hazard is identified, defined, and quantified (Step 1). For terrorism, the threat is the aggressors (people or groups) that are known to exist and that have the capability and a history of using hostile actions, or that have expressed intentions for using hostile actions against potential targets as well as on whom there is current credible information on targeting activity (surveillance of potential targets) or indications of preparation for terrorist acts. The capabilities and histories of the aggressors include the tactics they have used to achieve their ends. The next step of the assessment process is to identify the value of a building's assets that need to be protected (Step 2).

After conducting a asset value assessment, the next step is to conduct a vulner-

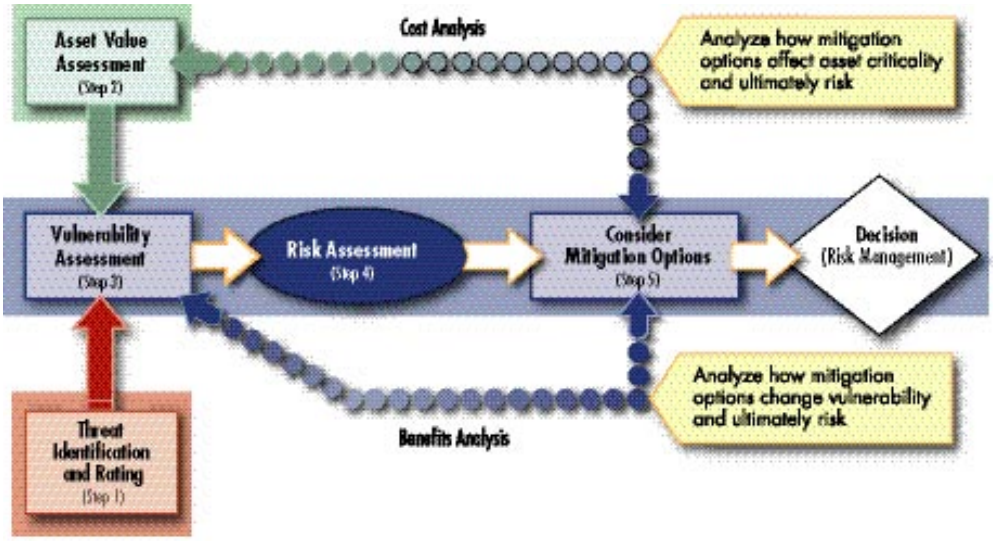


Figure 1 Risk assessment process model

ability assessment (Step 3). A vulnerability assessment evaluates the potential vulnerability of the critical assets against a broad range of identified threats/hazards. In and of itself, the vulnerability assessment provides a basis for determining mitigation measures for protection of the critical assets. The vulnerability assessment is the bridge in the methodology between threat/hazard, asset value, and the resultant level of risk.

The next step of the process is the risk assessment (Step 4). The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost mitigation measures, but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with the identified vulnerability, allow prioritization of resources to implement mitigation measures.

The final step (Step 5) is to consider mitigation options that are directly associated with, and responsive to, the major risks identified during Step 4. From Step 5, decisions can be made as to where to minimize the risks and how to accomplish that over time. This is commonly referred to as Risk Management.

A number of worksheets are utilized in this How-To Guide. They can be used to apply key concepts described in this document and are presented at the end of each Step.

A core element of this How-To Guide is the Building Vulnerability Assessment Checklist included in Appendix A. The Checklist can be used to collect and report information related to the building infrastructure. It 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. It allows a consistent security evaluation of designs at various levels.

A Risk Assessment Database accompanies this publication in the form of computer software. The purpose of this database is for a user to collect and organize risk scoring, building vulnerability data, and mitigation measures for multiple buildings. More information can be found throughout this publication and in Appendix B.

The Building Vulnerability Assessment Checklist and the Risk Assessment Database were developed for the Department of Veterans Affairs with assistance from the National Institute for Building Sciences.

ACKNOWLEDGMENTS

Principal Authors:

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

Eric Letvin, URS, Project Manager

Michael Chipley, PBSJ

Terrence Ryan, UTD, Inc.

Contributors:

Lloyd Siegel, Department of Veterans Affairs

Marcelle Habibion, Department of Veterans Affairs

Kurt Knight, Department of Veterans Affairs

Eve Hinman, Hinman Consulting Engineering

Bob Smilowitz, Weidlinger Associates Inc.

Stephanie King, Weidlinger Associates Inc.

Sarah Steerman, UTD, Inc.

Deb Daly, Greenhorne & O'Mara, Inc.

Julie Liptak, Greenhorne & O'Mara, Inc.

Wanda Rizer, Consultant

Project Advisory Panel:

Elizabeth Miller, National Capital Planning Commission

Doug Hall, Smithsonian Institution

Wade Belcher, General Service Administration

Michael Gressel, CDC/NIOSH

Kenneth Mead, CDC/NIOSH

Robert Chapman, NIST

Lawrence Skelly, Department of Homeland Security

Curt Betts, U.S. Army Corps of Engineers

Earle Kennett, National Institute for Building Sciences

Frederick Krimgold, Virginia Tech

David Hattis, Building Technology, Inc.

Ettore Contestabile, Canadian Explosives Research Laboratory

This How-To Guide was prepared under contract to FEMA. It will be revised periodically, and comments and feedback to improve future editions are welcome. Please send comments and feedback by e-mail to riskmanagementseriespubs@dhs.gov.

TABLE OF CONTENTS

Foreword and Acknowledgments i

Step 1: Threat Identification and Rating 1-1

Task 1.1 Identifying the Threats 1-1

Task 1.2 Collecting Information 1-16

Task 1.3 Selecting the Primary Threats 1-17

Task 1.4 Determining the Threat Rating 1-23

Step 2: Asset Value Assessment 2-1

Task 2.1 Identifying the Layers of Defense 2-2

Task 2.2 Identifying the Critical Assets 2-6

Task 2.3 Identifying the Building Core Functions and Infrastructure 2-17

Task 2.4 Determining the Asset Value Rating 2-23

Step 3: Vulnerability Assessment 3-1

Task 3.1 Organizing Resources to Prepare the Assessment 3-2

Task 3.2 Evaluating the Site and Building 3-6

Task 3.3 Preparing a Vulnerability Portfolio 3-11

Task 3.4 Determining the Vulnerability Rating 3-14

Step 4: Risk Assessment 4-1

Task 4.1 Preparing the Risk Assessment Matrices 4-2

Task 4.2 Determining the Risk Ratings 4-7

Task 4.3 Prioritizing Observations in the Building Vulnerability Assessment Checklist 4-10

Step 5: Consider Mitigation Options 5-1

Task 5.1 Identifying Preliminary Mitigation Options 5-2

Task 5.2 Reviewing Mitigation Options 5-6

Task 5.3 Estimating Cost 5-9

Task 5.4 Mitigation, Cost, and the Layers of Defense 5-13

Appendix A Building Vulnerability Assessment Checklist

Appendix B1 Risk Management Database: Assessor's User Guide

Appendix B2 Risk Management Database: Database Administrator's User Guide

Appendix B3 Risk Management Database: Manager's User Guide

Appendix C Acronyms and Abbreviations

Figures

Foreword and Acknowledgments

Figure 1 Risk assessment process model iii

Chapter 1

Figure 1-1 Steps and tasks 1-1

Figure 1-2 Total international attacks by region, 1998-2003 1-3

Figure 1-3 Explosive environments - blast range to effect 1-4

Figure 1-4 Incident overpressure as a function of stand-off distance 1-6

Figure 1-5 Total facilities affected by international terrorism and weapons of choice, 1998-2003 1-15

Chapter 2

Figure 2-1 Steps and tasks 2-1

Figure 2-2 Layers of defense 2-3

Figure 2-3 Layers of defense in an urban setting 2-5

Figure 2-4 Layers of defense when a particular building is considered a critical asset 2-5

Figure 2-5 Potential blast effects – 200-lb car bomb 2-7

Figure 2-6 Potential blast effects – 11,000-lb truck bomb 2-7

Figure 2-7 Using HAZUS-MH to identify the criticality of assets 2-8

Chapter 3

Figure 3-1 Steps and tasks..... 3-1

Figure 3-2 Common system vulnerabilities 3-15

Chapter 4

Figure 4-1 Steps and tasks..... 4-1

Chapter 5

Figure 5-1 Steps and tasks..... 5-1

Figure 5-2 Cost considerations..... 5-10

Figure 5-3 Mitigation options for the second layer of defense..... 5-14

Figure 5-4 Mitigation options for the third layer of defense 5-15

Tables

Chapter 1

Table 1-1 Explosive Evacuation Distance 1-5

Table 1-2 Critical Biological Agent Categories 1-11

Table 1-3 Event Profiles 1-13

Table 1-4 Criteria to Select Primary Threats..... 1-20

Table 1-5 Nominal Example to Select Primary Threats for a Specific Urban Multi-story Building..... 1-21

Table 1-6 Threat Rating..... 1-24

Table 1-7A Nominal Example of Threat Rating for an Urban Multi-story Building (Building Function) 1-25

Table 1-7B Nominal Example of Threat Rating for an Urban Multi-story Building (Building Infrastructure) 1-26

Chapter 2

Table 2-1 Correlation of the Layers of Defense Against Threats..... 2-12

Table 2-2 Building Core Functions..... 2-18

Table 2-3 Building Core Infrastructure..... 2-20

Table 2-4 Levels of Protection and Recommended Security Measures..... 2-21

Table 2-5 Asset Value Scale..... 2-23

Table 2-6A Nominal Example of Asset Value Rating for an Urban Multi-story Building (Building Function)..... 2-24

Table 2-6B Nominal Example of Asset Value Rating for an Urban Multi-story Building (Building Infrastructure)..... 2-24

Chapter 3

Table 3-1 Screening Phase..... 3-4

Table 3-2 Full On-site Evaluation..... 3-5

Table 3-3 Detailed Evaluation..... 3-5

Table 3-4 Vulnerability Rating..... 3-16

Table 3-5A Nominal Example of Vulnerability Rating for a Specific Multi-story Building (Building Function)..... 3-17

Table 3-5B Nominal Example of Vulnerability Rating for a Specific Multi-story Building (Building Infrastructure)..... 3-17

Chapter 4

Table 4-1 Critical Functions Asset Value..... 4-4

Table 4-2 Critical Infrastructure Asset Value..... 4-4

Table 4-3 Critical Functions Threat Rating..... 4-5

Table 4-4 Critical Infrastructure Threat Rating..... 4-5

Table 4-5 Critical Functions Vulnerability Rating..... 4-6

Table 4-6 Critical Infrastructure Vulnerability Rating..... 4-7

Table 4-7 Total Risk Scale Color Code..... 4-8

Table 4-8 Site Functional Pre-Assessment Screening Matrix..... 4-8

Table 4-9 Site Infrastructure Pre-Assessment Screening Matrix..... 4-9

Table 4-10 Nominal Example of Observations in the Building Vulnerability Assessment Checklist..... 4-10

STEP 1: THREAT IDENTIFICATION AND RATING

OVERVIEW

The first step in the assessment process is to help you to identify threats that are a priority concern in your area and that may pose a risk to your assets (see Figure 1-1). The threat identification and rating process involves the following tasks:

- Identifying the threats
- Collecting information
- Determining the design basis threat
- Determining the threat rating

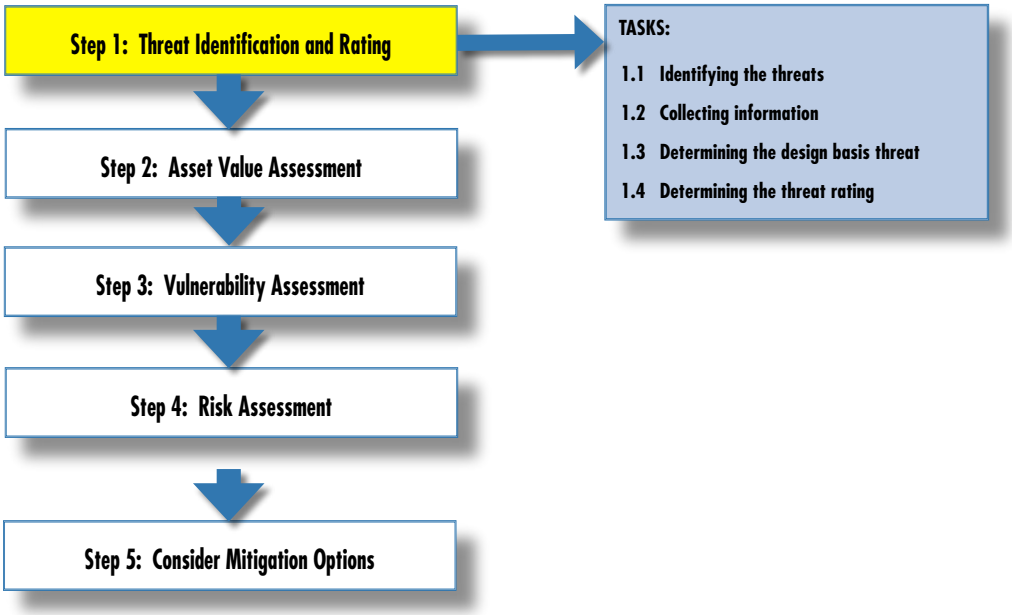


Figure 1-1 Steps and tasks

Identifying the Threats (Task 1.1)

For this document, threat is defined as any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. Within the military services, the intelligence community, and law enforcement, the term "threat" is typically used to describe the design criteria for terrorism or manmade disasters. The Federal Emergency Management Agency (FEMA) and other civil agencies use the term "hazard" in several different contexts. "Natural hazard" typically refers to a natural event such as a flood, wind, or seismic disaster.

"Human-caused (or manmade) hazards" are "technological hazards" and "terrorism" and are distinct from natural hazards primarily in that they originate from human activity. "Technological hazards" (i.e., a HazMat leak from a railcar) are generally assumed to be accidental and that their consequences are unintended. (Note that protection against technological hazards can also serve for the protection against terrorist attacks.) "Terrorism" is considered an unlawful act 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.

In this guide, only manmade terrorist threats will be used in the critical functions and infrastructure matrices. The importance of technological hazards is that they can become a threat if they are targets of malicious attacks.

Identifying the threats can be a difficult task. Because manmade hazards are different from other hazards such as earthquakes, floods, and hurricanes, they are difficult to predict. Many years of historical and quantitative data, and probabilities associated with the cycle, duration, and magnitude of natural hazards exist. The fact that data for manmade hazards are scarce and that the magnitude and recurrence of terrorist attacks are almost unpredictable makes the determination of a particular threat for any particular site or building difficult and largely subjective.

With any terrorist threats, it is important to understand who the people are with the intent to cause harm. The aggressors seek publicity for their cause, monetary gain (in some instances), or political gain through their actions. These actions include injuring or killing people; destroying or damaging facilities, property, equipment, or resources; or stealing equipment, material, or information. In some cases, the threat may originate from more than one group, with differing methods and motives.

Aggressor tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; bombs delivered by persons (suicide bombers); exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed bombs); attack weapons (rocket propelled grenades, light antitank weapons, etc.); ballistic attacks (small arms handled by one individual); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals); supply bombs (larger bombs processed through shipping departments); airborne contamination (chemical, biological, or radiological [CBR] agents used to contaminate the air supply of a building); and waterborne contamination (CBR agents injected into the water supply).

Domestic terrorism refers to activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States.

International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; affect the conduct of a government by mass destruction, assassination or kidnapping; and occur primarily outside the territorial jurisdiction of the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. Totals for international terrorism in 1998-2003 are shown by regions in Figure 1-2.

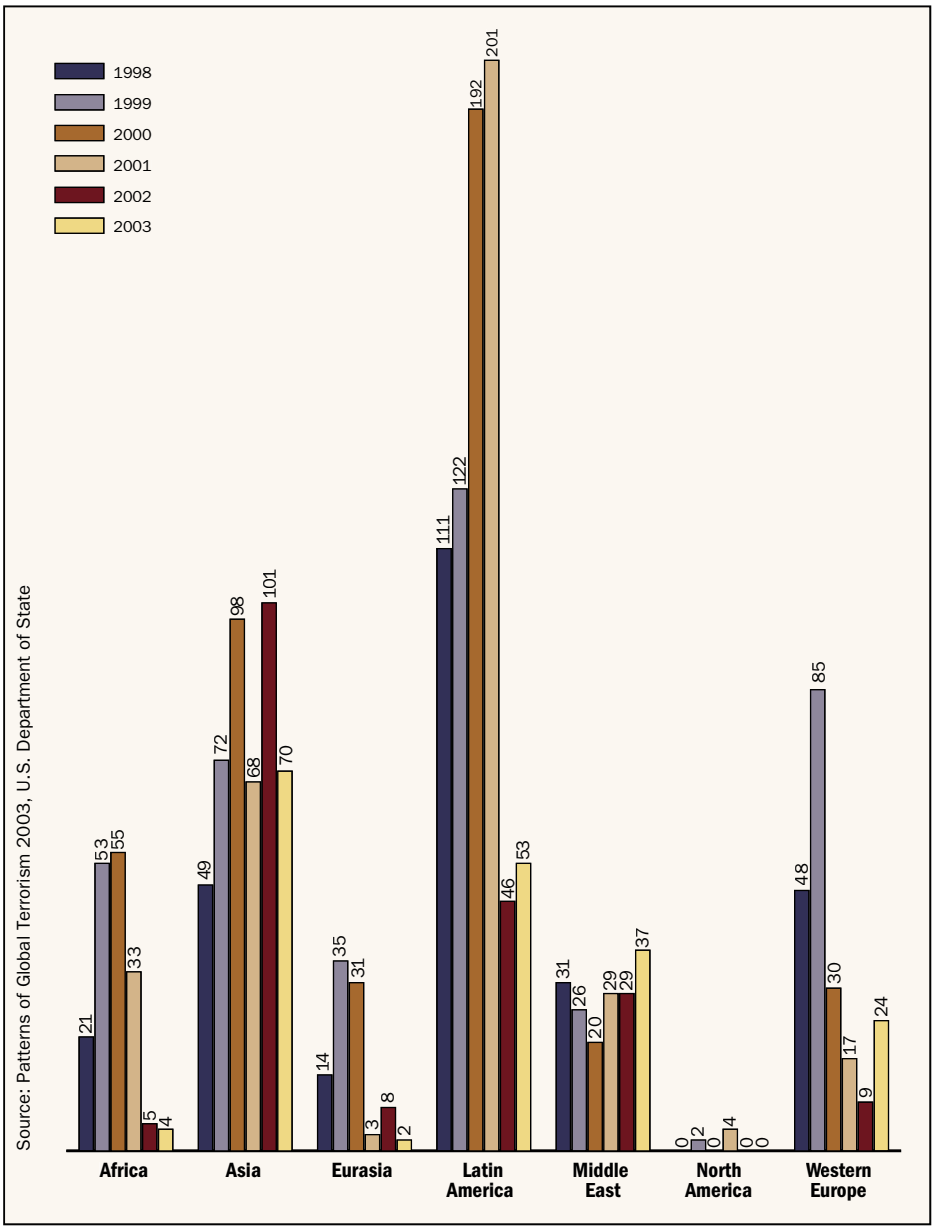


Figure 1-2 Total international attacks by region, 1998-2003

Explosive Blast Weapons

Two parameters are used to define the explosive blast design threat: the weapon size, measured in equivalent pounds of trinitrotoluene (TNT), and the stand-off. The stand-off is the distance measured from the center of gravity of the charge to the component of interest.

Figures 1-3, 1-4, and Table 1-1 illustrate these principles. Figure 1-3 shows an example of a blast range-to-effect chart that indicates the distance or stand-off to which a given size bomb will produce a given effect. Table 1-1 is a quick reference chart that provides recommended evacuation distances for a given explosive weight. Figure 1-4 provides a quick method for predicting the expected overpressure (expressed in pounds per square inch or psi) on a building for a specific explosive weight and stand-off distance. For additional information on overpressure and blast effects, see FEMA 426 and 427.

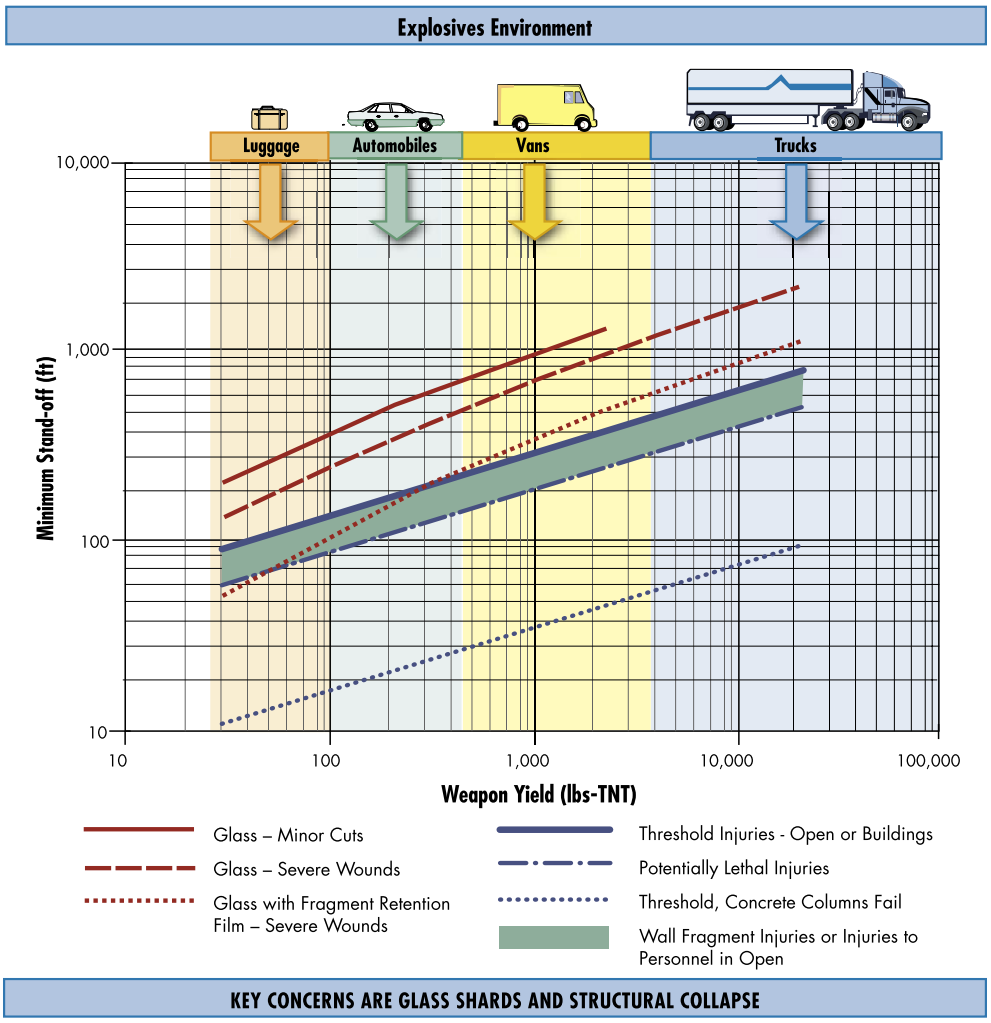


Figure 1-3 Explosive environments - blast range to effect

Table 1-1 Explosive Evacuation Distance

	Threat Description	Explosive Mass[1] (TNT Equivalent)	Building Evacuation Distance[2]	Outdoor Evacuation Distance[3]
High Explosives (TNT Equivalent)	Pipe Bomb	5 lbs 2.3 kg	70 ft 21 m	850 ft 259 m
	Suicide Belt	10 lbs 4.5 kg	90 ft 27 m	1,080 ft 330 m
	Suicide Vest	20 lbs 9 kg	110 ft 34 m	1,360 ft 415 m
	Briefcase/Suitcase Bomb	50 lbs 23 kg	150 ft 46 m	1,850 ft 564 m
	Compact Sedan	500 lbs 227 kg	320 ft 98 m	1,500 ft 457 m
	Sedan	1,000 lbs 454 kg	400 ft 122 m	1,750 ft 534 m
	Passenger/Cargo Van	4,000 lbs 1,814 kg	640 ft 195 m	2,750 ft 838 m
	Small Moving Van/Delivery Truck	10,000 lbs 4,536 kg	860 ft 263 m	3,750 ft 1,143 m
	Moving Van/Water Truck	30,000 lbs 13,608 kg	1,240 ft 375 m	6,500 ft 1,982 m
	Semitrailer	60,000 lbs 27,216 kg	1,570 ft 475 m	7,000 ft 2,134 m

[1]*Based on the maximum amount of material that could reasonably fit into a container or vehicle. Variations are possible.*

[2]*Governed by the ability of an unreinforced building to withstand severe damage or collapse.*

[3]*Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. These distances can be reduced for personnel wearing ballistic protection. Note that the pipe bomb, suicide belt/vest, and briefcase/suitcase bomb are assumed to have a fragmentation characteristic that requires greater stand-off distances than an equal amount of explosives in a vehicle.*

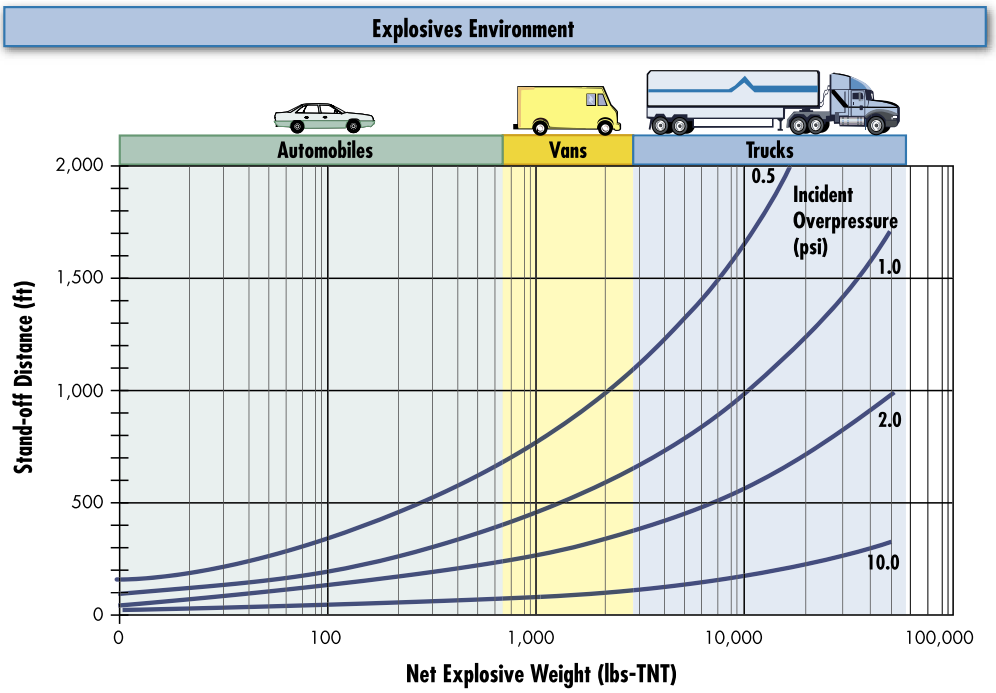


Figure 1-4 Incident overpressure as a function of stand-off distance

To put the weapon size into perspective, it should be noted that thousands of explosions occur every year within the United States, but the vast majority of them have weapon yields of less than 5 pounds. The number of large-scale vehicle weapon attacks that have used hundreds of pounds of TNT during the past 20 years is, by comparison, very small. In general, the largest credible explosive size is a function of the security measures in place. Each line of security may be thought of as a sieve, reducing the size of the weapon that may gain access. Therefore, the largest weapons are considered in totally unsecured public spaces (e.g., in a vehicle on the nearest public street), and the smallest weapons are considered in the most secured areas of the building (e.g., in a briefcase smuggled past the screening station). It should also be noted that the likely target is often not the building under consideration by the risk assessment, but a high-risk building that is nearby. Historically, more building damage has been due to collateral effects than direct attack. Based upon access to the agent, the degree of difficulty, and past experience, it can be stated that the chance of a large-scale explosive attack occurring is extremely low and that a smaller explosive attack is far more likely.

From the standpoint of structural design, the vehicle bomb is the most important consideration and has been a favorite tactic of terrorists. Ingredients for homemade bombs are easily obtained on the open market, as are the techniques for making bombs.

Vehicle bombs are able to deliver a sufficiently large quantity of explosives to cause potentially devastating structural damage. Security design intended to limit or mitigate damage from a vehicle bomb assumes that the bomb is detonated at a so-called critical location. The critical location is a function of the site, the building layout, the security measures in place, and the position of the weapon. For a vehicle bomb, the critical location is taken to be at the closest point that a vehicle can approach, assuming that all security measures are in place. This may be a parking area directly beneath the occupied building, the loading dock, the curb directly outside the facility, or at a vehicle-access control gate where inspection takes place, depending on the level of protection incorporated into the design.

Another explosive attack threat is the small bomb that is hand delivered. Small weapons can cause large damage when they are brought into vulnerable and unsecured areas of the building. Greater damage may be caused when the weapon is brought into the interior, such as the building lobby, mail room, and retail spaces. Recent events around the world make it clear that there is an increased likelihood that bombs will be delivered by persons (suicide bombers or hand carried bombs) who are willing to sacrifice their own lives. Hand-carried explosives are typically on the order of 5 to 10 pounds of TNT equivalent. However, larger charge weights, in the 50- to 100-pound TNT equivalent range, can be readily carried in rolling cases. Mail bombs are typically less than 10 pounds of TNT equivalent.

For design purposes, large-scale truck bombs typically contain 10,000 pounds or more of TNT equivalent, depending on the size and capacity of the vehicle used to deliver the weapon. Vehicle bombs that utilize vans down to small sedans typically contain 5,000 to 100 pounds of TNT equivalent, respectively. A briefcase bomb is approximately 50 pounds, and a pipe bomb is generally in the range of 5 pounds of TNT equivalent. Suicide bombers can deliver belts ranging from 10 pounds (teenagers), 15 to 20 pounds (women), and 30 to 40 pounds (men).

Chemical, Biological, and Radiological Weapons

Three parameters are used to define the CBR design basis threat: the exposure, the duration, and the concentration. Each of the CBR agents has different human effects and methods of attack.

Chemical, biological, and radiological attacks are an emerging threat and of great concern because of the large geographic area contaminated, numbers of people affected, and the high economic cost of response and recovery. The use of CBR weapons and the stated intent of terrorist groups to acquire and use the weapons increases the target set, and the weapons can affect a single building, an entire city, multiple counties, or even states.

Like explosive threats, CBR threats may be delivered externally or internally to the building. External ground-based threats may be released at a stand-off distance from the building or may be delivered directly through an air intake or other opening. Interior threats may be delivered to accessible areas such as the lobby, mailroom, loading dock, or egress route. Because there may not be an official or obvious warning prior to a CBR event, the best defense is to be alert to signs of a release occurring.

Chemical. Chemical agents are compounds with unique chemical properties that can produce lethal or damaging effects in humans, animals, and plants. Chemical agents can exist as solids, liquids, or gases, depending on temperature and pressure. Most chemical agents are liquid and can be introduced into an unprotected population relatively easily using aerosol generators, explosive devices, breaking containers, or other forms of covert dissemination. Dispersed as an aerosol or vapor, chemical agents have their greatest potential for inflicting mass casualties. There are two categories of chemicals: lethal and incapacitating. The lethal chemicals are subdivided into industrial and warfare.

Industrial chemicals are used extensively throughout the nation on a daily basis. Lethal industrial chemicals are listed as Toxic Industrial Compounds (TICs). Of concern is the use of TICs as a weapon (e.g., derailment of a chlorine tanker car), especially in the urban environment.

Chemical agents can have an immediate effect (a few seconds to a few minutes) or a delayed effect (several hours to several days). Although potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly. Chemical agents are also difficult to produce. There are six types of agents:

- Choking/lung-damaging (pulmonary) agents such as chlorine and phosgene
- Blood agents such as cyanide
- Vesicants or blister agents such as mustard
- Nerve agents such as GA (tabun), GB (sarin), GD (soman), GF (cyclohexyl sarin), and VX (phosphonothioic acid)
- Incapacitating agents such as BZ (3-quinulidinyle benzilate)
- Riot-control agents similar to Mace

Biological. Biological agents pose a serious threat, but most are difficult to grow and maintain. These agents are disseminated by the use of aerosols, contaminated food or water supplies, direct skin contact, or injection. Several biological agents can be adapted for use as weapons by terrorists. These agents include anthrax (sometimes found in sheep and cattle), tularemia (rabbit fever), cholera, the plague (sometimes found in prairie dog colonies), and botulism (found in improperly canned food). A biological incident will most likely be first recognized in the hospital emergency room, medical examiner's office, or within the public health community long after the terrorist attack. The consequences of such an attack may present communities with an unprecedented requirement to provide mass protective treatment to exposed populations, mass patient care, mass fatality management, and environmental health cleanup procedures and plans.

Biological agents are organisms or toxins that can kill or incapacitate people, livestock, and crops. The three basic groups of biological agents that would likely be used as weapons are bacteria, viruses, and toxins.

1. Bacteria are small free-living organisms that reproduce by simple division and are easy to grow. The diseases they produce often respond to treatment with antibiotics.

2. Viruses are organisms that require living cells in which to reproduce and are intimately dependent upon the body they infect. Viruses produce diseases that generally do not respond to antibiotics; however, antiviral drugs are sometimes effective.

3. Toxins are poisonous substances found in, and extracted from, living plants, animals, or microorganisms; some toxins can be produced or altered by chemical means. Some toxins can be treated with specific antitoxins and selected drugs.

Many biological agents break down quickly when exposed to sunlight and other environmental factors, while others such as anthrax spores are very long lived. They can be dispersed by spraying them in the air, or by infecting animals or humans, as well through food and water contamination.

- **Aerosols —** Biological agents are dispersed into the air as an aerosol that may drift for miles. Inhaling the agent may cause disease in people or animals.

- **Animals —** Some diseases are spread by insects and animals, such as fleas,

mice, flies, and mosquitoes. Deliberately spreading diseases through livestock is also referred to as agro-terrorism.

- **Food and water contamination —** Some pathogenic organisms and toxins may persist in food and water supplies. Most microbes can be killed, and toxins deactivated, by cooking food and boiling water.

Person-to-person spread of a few infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and the Lassa viruses. In a 2002 report, Public Health Assessment of Biological Terrorism Agents, the Centers for Disease Control (CDC) has classified biological agents as one of three priority categories for initial public health preparedness efforts: A, B, or C (see Table 1-2). The CDC maintains a comprehensive list of agents, diseases, and other threats at www.bt.cdc.gov/agent/index.asp.

Agents in Category A have the greatest potential for adverse public health impact with mass casualties, and most require broad-based public health preparedness efforts (e.g., improved surveillance and laboratory diagnosis and stockpiling of specific medications). Category A agents also have a moderate to high potential for large-scale dissemination or a heightened general public awareness that could cause mass public fear and civil disruption.

Most Category B agents also have some potential for large-scale dissemination with resultant illness, but generally cause less illness and death, and, therefore, would be expected to have lower medical and public health impacts. These agents also have lower general public awareness than Category A agents and require fewer special public health preparedness efforts. Agents in this category require some improvement in public health and medical awareness, surveillance, or laboratory diagnostic capabilities, but present limited additional requirements for stockpiled therapeutics beyond those identified for Category A agents. Biological agents that have undergone some development for widespread dissemination but do not otherwise meet the criteria for Category A, as well as several biological agents of concern for food and water safety, are included in this category.

Biological agents that are currently not believed to present a high bioterrorism risk to public health, but that could emerge as future threats (as scientific understanding of these agents improves) were placed in Category C.

Table 1-2: Critical Biological Agent Categories

Biological Agent(s)	Disease
Category A	
Variola major	Smallpox
Bacillus anthracis	Anthrax
Yersinia pestis	Plague
Clostridium botulinum (botulinum toxins)	Botulism
Francisella tulaensis	Tularemia
Filoviruses and Arenaviruses (e.g., Ebola virus, Lassa virus)	Viral hemorrhagic fevers
Category B	
Coxiella burnetii	Q fever
Brucella spp.	Brucellosis
Burkholderia mallei	Glanders
Burkholderia pseudomallei	Meliodosis
Alphaviruses	Encephalitis
Rickettsia prowazekii	Typhus fever
Toxins (e.g., Ricin)	Toxic syndromes
Chlamydia psittaci	Psittacosis
Food safety threats (e.g., *Salmonella spp.*)	
Water safety threats (e.g., *Vibrio cholerae*)	
Category C	
Emerging threat agents (e.g., *Nipah virus*, hantavirus)	

SOURCE: PUBLIC HEALTH ASSESSMENT OF POTENTIAL BIOLOGICAL TERRORISM AGENTS (CDC, 2002)

Nuclear and Radiological. Nuclear threat is the use, threatened use, or threatened detonation of a nuclear bomb or device. At present, there is no known instance in which any non-governmental entity has been able to obtain or produce a nuclear weapon. The most likely scenario is the detonation of a large conventional explosive that incorporates nuclear material or detonation of an explosive proximate to nuclear materials in use, storage, or transit. Of concern is the increasing frequency of shipments of radiological materials throughout the world.

Nuclear explosions can cause deadly effects: blinding light, intense heat (thermal radiation), initial nuclear radiation, blast, fires started by the heat pulse, and secondary fires caused by the destruction. They also produce radioactive particles called fallout that can be carried by wind for hundreds of miles.

Terrorist use of a radiological dispersion device (RDD) – often called ”dirty nuke” or “dirty bomb” – is considered far more likely than the use of a nuclear device. These radiological weapons are a combination of conventional explosives and radioactive material designed to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Such radiological weapons appeal to terrorists because they require very little technical knowledge to build and deploy compared to that of a nuclear device. Also, these radioactive materials, used widely in medicine, agriculture, industry, and research, are much more readily available and easy to obtain compared to weapons grade uranium or plutonium.

There is no way of knowing how much warning time there would be before an attack by a terrorist using a nuclear or radiological weapon. A surprise attack remains a possibility. The danger of a massive strategic nuclear attack on the United States involving many weapons receded with the end of the Cold War; however, some terrorists have been supported by nations that have nuclear weapons programs.

Other Threats. Other threats discussed in this manual include armed attacks, cyber attacks, high-altitude electromagnetic pulse, and high power microwave. These are discussed briefly in Table 1-3.

Table 1-3 provides selected threats that you may consider when preparing your risk assessment, some of which has not been discussed previously in this How-To Guide.

Table 1-3: Event Profiles

Threat	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Improvised Explosive Device (Bomb) - Stationary Vehicle - Moving Vehicle - Mail - Supply - Thrown - Placed - Suicide Bomber	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Blast energy at a given stand-off is inversely proportional to the cube of the distance from the device; thus, each additional increment of stand-off provides progressively more protection. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
Armed Attack - Ballistics (small arms) - Stand-off Weapons (rocket propelled grenades, mortars)	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator's intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.
Chemical Agent - Blister - Blood - Choking/Lung/ Pulmonary - Incapacitating - Nerve - Riot Control/Tear Gas - Vomiting	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/ containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation in pools of liquids. Humidity can enlarge aerosol particles, reducing the inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect people and property from harmful effects for a limited time.

Table 1-3: Event Profiles (continued)

Threat	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Biological Agent - Anthrax - Botulism - Brucellosis - Plague - Smallpox - Tularemia - Viral Hemorrhagic Fevers - Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins)	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents, but higher winds can break up aerosol clouds; and the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.
Radiological Agent - Alpha - Beta - Gamma	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
Cyber Attacks	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.
High-Altitude Electromagnetic Pulse (HEMP)	An electromagnetic energy field produced in the atmosphere by the power and radiation of a nuclear explosion. It can overload computer circuitry with effects similar to, but causing damage much more swiftly than a lightning strike.	It can be induced hundreds to a few thousand kilometers from the detonation.	Affects electronic systems. There is no effect on people. It diminishes with distance, and electronic equipment that is turned off is less likely to be damaged.	To produce maximum effect, a nuclear device must explode very high in the atmosphere. Electronic equipment may be hardened by surrounding it with protective metallic shielding that routes damaging electromagnetic fields away from highly sensitive electrical components.

Table 1-3: Event Profiles (continued)

Threat	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
High Power Microwave (HPM) EMP	It is a non-nuclear radio frequency energy field. Radio frequency weapons can be hidden in an attaché case, suitcase, van, or aircraft. Energy can be focused using an antenna, or emitter, to produce effects similar to HEMP, but only within a very limited range.	An HPM weapon has a shorter possible range than HEMP, but it can induce currents large enough to melt circuitry, or it can cause equipment to fail minutes, days, or even weeks later. HPM weapons are smaller-scale, are delivered at a closer range to the intended target, and can sometimes be emitted for a longer duration.	Vulnerable systems include electronic ignition systems, radars, communications, data processing, navigation, electronic triggers of explosive devices. HPM capabilities can cause a painful burning sensation or other injury to a person directly in the path of the focused power beam, or can be fatal if a person is too close to the microwave emitter.	Very damaging to electronics within a small geographic area. A shockwave could disrupt many computers within a 1-mile range. Radio frequency weapons have ranges from tens of meters to tens of kilometers. Unlike HEMP, however, HPM radiation is composed of shorter wave forms at higher-frequencies, which make it highly effective against electronic equipment and more difficult to harden against.

Note: Cyber attack focuses on denial of service, worms, and viruses designed to attack or destroy critical infrastructure related systems such as energy management, supervisory control and data acquisition systems, security, control valves, and voice over internet protocol telephones, which are critical systems that support multiple functions and are becoming increasingly connected to the internet.

It is important to indicate that commercial buildings have been the preferred target of recent terrorist attacks. Figure 1-5 illustrates such actions. Between 1998 and 2003, 1,566 commercial facilities were struck by terrorists while only 97 government, 170 diplomat facilities, and 41 military facilities were affected during the same period.

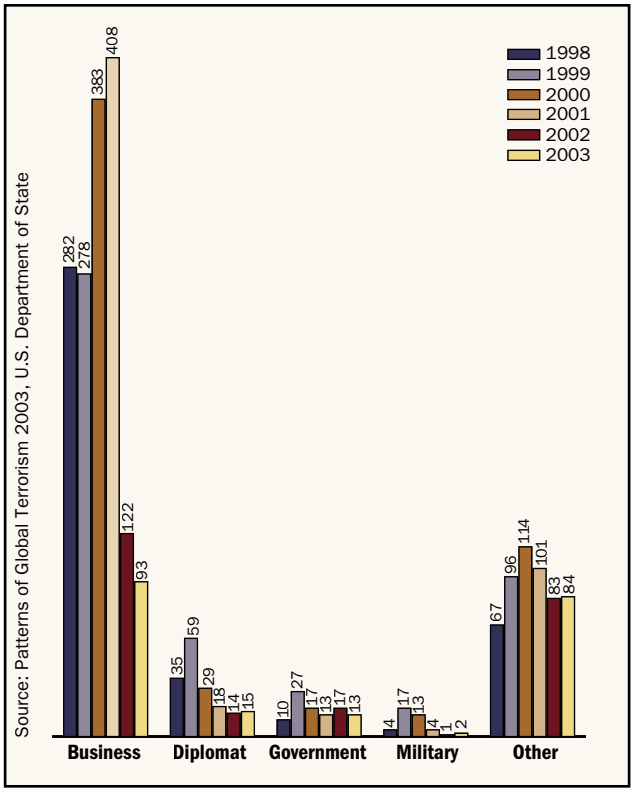


Figure 1-5 Total facilities affected by international terrorism and weapons of choice, 1998-2003

Collecting Information (Task 1.2)

When collecting information for your threat assessment, you may ask the following questions: What groups or organizations exist/are known? Do they have capability among themselves or is that capability readily obtainable locally? Do they have a history of terrorist acts and what are their tactics? What are the intentions of the aggressors against the government, commercial enterprises, industrial sectors, or individuals? Has it been determined that targeting (planning a tactic or seeking vulnerabilities) is actually occurring or being discussed?

For technological hazards, these same questions take a different perspective. Does anything that can be a hazard (or be attacked, causing collateral damage) exist within a given distance of the building in question? What is the capability of that incident to cause harm? Is there a history of this type of accident occurring?

Many security and intelligence organizations are a good source of information and data for threat assessments. These organizations include the police department (whose jurisdiction includes the building or site), the local State police office, and the local office of the Federal Bureau of Investigation (FBI.) In many areas of the country, there are threat coordinating committees, including FBI Joint Terrorism Task Forces, that facilitate the sharing of information. In addition, the CDC, the U.S. Department of Homeland Security (DHS), and the Homeland Security Offices (HSOs) at the State level are good sources of information. For technological hazards, it is 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.

Other good sources of information include the Department of Homeland Security Information Analysis and Infrastructure Protection (IA/IP) Directorate and, under the Director, Central Intelligence Agency (CIA), the Terrorist Threat Integration Center (TTIC). The IA/IP Directorate and the TTIC enhance intelligence fusion to bring together all terrorist information

in one place, enabling America's best intelligence analysts and investigators from multiple departments to work as a team to put together the pieces of the puzzle.

Threat information is communicated through The Homeland Security Information Network. This communications system delivers real-time interactive connectivity among State and local partners and with the DHS Homeland Security Operations Center (HSOC) through the Joint Regional Information Exchange System (JRIES). Other DHS agencies participate through seats at the HSOC and their own operations centers, and the system will be further expanded within DHS operations. Each State and major urban area's Homeland Security Advisor and other points of contact will receive software licenses, technology, and training to participate in the information sharing and situational awareness that JRIES already brings to State and local homeland security personnel across the United States. Examples of other points of participation include State National Guard offices, Emergency Operations Centers (EOCs), and first responder and Public Safety departments.

The network significantly strengthens the flow of real-time threat information to State, local, and private sector partners at the Sensitive-but-Unclassified level (SBU), and provides a platform for communications through the classified SECRET level to State offices. The program is built upon the JRIES platform, a secure network and a suite of applications currently operating at the SBU level. Participants currently include approximately 100 organizations, including Federal agencies, States, municipalities, and other local government entities, with a significant law enforcement user base. All participating entities have a certified counterterrorism mission. Approximately 1,000 users currently have access to the system.

Selecting the Primary Threats (Task 1.3)

Stopping a terrorist or physical attack on a building is very difficult; any building or site can be breached or destroyed. Weapons, tools, and tactics can change faster than a building can be modified against a particular threat. However, the more secure the building or site and the better the building is designed to withstand an attack, the better the odds the building will not be attacked or, if attacked, it will suffer less damage. Terrorists generally select targets that have some value as a target, such as an iconic commercial property, symbolic government building, or structure likely to inflict significant emotional or economic damage such as a shopping mall or major seaport.

The type and size of the weapons to be considered in the threat assessment

are usually selected by the building stakeholders in collaboration with the Assessment Team (i.e., engineers who specialize in the design of structures to mitigate the effects of explosions - see Step 3 of this How-To Guide). The threat assessment and analysis for any building can range from a general threat scenario to a very detailed examination of specific groups, individuals, and tactics that the building may need to be designed to repel or defend against. For this How-To Guide, a simplified method has been selected to help the Assessment Team and building stakeholders to identify the primary threats to their buildings (see Approach to Selecting Primary Threats below and Table 1-4).

Users of this How-to-Guide should understand that tables provided in this step (Tables 1.4 and 1.5) are only a brainstorming tool and should not be used to conduct a comprehensive threat assessment or set design criteria for new or existing buildings. Methods for performing a comprehensive threat assessment include the following: TM5-853 Army-Air Force Security Engineering Manual, the State of Florida HLS-CAM vulnerability and criticality matrix, the Department of Defense (DoD) CARVER process, and the FEMA 386-7 Site/Building Inherent Vulnerability Assessment Matrix. The determination of which method to be used should be left to the Assessment Team and building owners.

Approach to Selecting Primary Threats

Unlike natural disasters, terrorists continually evaluate, plan, and seek to exploit the weakest building protective design features. Therefore, it becomes impossible both from a technical and benefit/cost point to try to protect everything from every type of attack. The building stakeholders have to make a determination as to what the design basis threat is for their building and what level of protection they can afford. As the terrorist threat changes over time, the building stakeholders may wish to revisit this part of the risk assessment process.

To select your primary threats for the risk assessment, the criteria described below have been provided. The selected criteria are part of Table 1-4, which is designed to help you to determine your potential threats. Scores from 1 to 10 (10 being the greater threat) are described. It should be noted that for a single building, many of the scores for these criteria may be the same. The scores would change when assessing multiple buildings.

- **Access to Agent.** The ease by which the source material can be acquired to carry out the attack. Consideration includes the local materials of 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 arm an agent) and the technical knowledge of the systems to be attacked (heating, ventilation, and air conditioning [HVAC], nuclear, etc.). Knowledge and expertise can be gained by surveillance, open source research, specialized training, or years of practice in industry.

- **History of Threats (Building Functions/Tenants).** What has the potential threat element done in the past, how many times, and was the threat local, regional, national, or international in nature? When was the most recent incident and where, and against what target? Are the building functions and tenants attractive targets for the terrorist?

- **Asset Visibility/Symbolic.** The economic, cultural, and symbolic importance of the building to society that may be exploited by the terrorist seeking 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.** The level of defense currently offered by the building against each of the potential threats. This should be defined based on the degree security was considered in the original design of the building and any subsequent actions taken to minimize the impact of potential threats.

Table 1-4 is used in conjunction with Table 1-3 to create a general Threat Scenario for the site or building. Table 1-5 illustrates the use of the threat scoring matrix for a typical multi-story commercial office building in an urban area with underground parking, internet enabled environmental energy management system, Voice over Internet Protocol (VoIP) telecommunications system, Internal Protocol/Transmission Control Protocol (IP/TCP) enabled security system using local area network (LAN) and wireless connectivity for closed-circuit televisions (CCTVs) and entry access control, and standard hard wire

connectivity for the fire alarm system. Your potential threats will be selected from those reaching the highest scores.

Table 1-4: Criteria to Select Primary Threats

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.

Table 1-5: Nominal Example to Select Primary Threats for a Specific Urban Multi-story Building

Criteria								Score
Scenario		**Access to Agent**	**Knowledge/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Level of Defense**	
Improvised Explosive Device (Bomb)									
1-lb. Mail Bomb		9	9	3	8	3	10	3	45
5-lb. Pipe Bomb		9	9	3	8	3	10	3	45
50-lb. Satchel Bomb/Suicide Bomber		8	8	6	8	3	10	5	48
500-lb. Car Bomb		6	8	7	8	3	10	5	47
5,000-lb. Truck Bomb		4	8	5	8	3	10	3	41
20,000-lb. Truck Bomb		2	6	1	8	3	10	3	33
Natural Gas		2	8	1	8	3	10	5	37
Bomb/Aircraft/Ship									
Small Aircraft		9	6	3	8	3	10	5	44
Medium Aircraft		5	4	7	8	3	10	6	43
Large Aircraft		2	3	7	8	3	10	7	40
Ship		0	0	0	8	3	10	8	29
Chemical Agent									
Choking	Chlorine	5	7	2	8	3	10	5	40
	Phosgene	3	10	2	8	3	10	5	41
Blood	Hydrogen Cyanide	3	8	2	8	3	10	5	39
Blister	Lewisite	3	6	2	8	3	10	5	37
Nerve	Sarin	3	4	9	8	3	10	5	42

Table 1-5: Nominal Example to Select Primary Threats for a Specific Urban Multi-story Building (continued)

Scenario		Criteria							Score
		Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense	
Biological Agent									
Bacteria	Anthrax	4	5	9	8	3	10	5	44
	Plague	4	5	3	8	3	10	5	38
	Tularemia	4	5	2	8	3	10	5	37
Viruses	Hemorrehagic Fevers	4	5	2	8	3	10	5	37
	Smallpox	2	5	2	8	3	10	5	35
Toxins	Botulinum	5	5	5	8	3	10	5	41
	Ricin	8	8	9	8	3	10	5	51
Radiological Agent									
"Dirty Bomb"		5	7	1	8	3	10	7	41
Spent Fuel Storage		2	6	1	8	3	10	7	37
Nuclear Plant		1	6	1	8	3	10	7	36
Armed Attack									
RPG/LAW/Mortar		4	5	2	8	3	10	4	36
Ballistic		10	10	2	8	3	10	4	47
Cyber Attack									
Worm		9	10	5	8	3	10	4	49
Virus		9	10	5	8	3	10	4	49
Denial of Service		9	7	5	8	3	10	4	46

Note that the values for "Asset Visibility/Symbolic," "Asset Accessibility," and "Site Population/Capacity" are constants because a single building is being analyzed.

For the nominal example, the five primary threats that will be examined include:

- **Vehicle Bomb.** 500-lb. car bomb detonating within 15 feet of building exterior
- **Suicide Bomber.** An individual with a 50-lb. improvised explosive device
- **Chemical Agent.** Sarin gas most toxic of the listed agents; assumed worst case
- **Biological Agent.** Recent mail attacks with Ricin; no antidote, high economic productivity loss
- **Cyber Attack.** Impact on Emergency Management Systems (EMS), VoIP telecommunications, security systems

The "dirty bomb" and armed assault are other potential threats that could be considered, but are left out of this analysis for simplicity.

Note that the selection of the primary threats, as illustrated in this nominal example, is subjective and typically includes judgment on the part of the building stakeholders and the Assessment Team to evaluate the summed scores. As shown in Table 1-5, it is possible that the range in scores among the potential threats may be relatively narrow for a given building. To complete this portion of the risk assessment, you should use Worksheet 1-1 to provide a first level analysis of the primary threats that may affect your site or building.

Determining the Threat Rating (Task 1.4)

Having selected the primary threats for your site or 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.

For determining the threat rating, this How-To Guide provides a methodology based on consensus opinion of the building stakeholders, threat specialists, and engineers. (This group could be expanded as necessary to help refine the scoring process.) Table 1-6 provides a scale to help you with

this process. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). The key elements of this scale are the likelihood/credibility of a threat, potential weapons to be used during a terrorist attack, and information available to decision-makers. 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 a primary threat attack occur. Tables 1-7A and 1-7B display a nominal example of applying these ratings for an urban multi-story building.

Table 1-6: Threat Rating

Threat Rating		
Very High	10	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	8-9	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium High	7	Medium High – The likelihood of a threat, weapon, and tactic being used against the site or building is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium	5-6	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
Medium Low	4	Medium Low – The likelihood of a threat, weapon, and tactic being used in the region is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not likely.
Low	2-3	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

Worksheet 1-2 helps you organize and determine the threat rating in terms of building functions and infrastructure (see Task 2.3). The purpose is to produce a more informed opinion regarding the manmade hazards that affect your assets.

As a starting point, use a value of 5 and assume a medium level of threat; then adjust the threat rating up or down based on consensus. Note that the threat rating is independent of the building function and infrastructure because it is assumed to be ubiquitous to the entire building and the same threat numeric value is used vertically for each function or infrastructure component (see Tables 1-7A and 1-7B). For the purposes of this nominal example, selected threats from Table 1-5 were chosen. Since its a nominal example, scores are illustrative only.

Table 1-7A: Nominal Example of Threat Rating for an Urban Multi-story Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	8	4	5	2	2
Engineering	8	4	5	2	2
Warehousing	8	4	5	2	2
Data Center	8	4	5	2	2
Food Service	8	4	5	2	2
Security	8	4	5	2	2
Housekeeping	8	4	5	2	2
Day Care	8	4	5	2	2

Table 1-7B: Nominal Example of Threat Rating for an Urban Multi-story Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	8	4	5	2	2
Architectural	8	4	5	2	2
Structural Systems	8	4	5	2	2
Envelope Systems	8	4	5	2	2
Utility Systems	8	4	5	2	2
Mechanical Systems	8	4	5	2	2
Plumbing and Gas Systems	8	4	5	2	2
Electrical Systems	8	4	5	2	2
Fire Alarm Systems	8	4	5	2	2
IT/Communications Systems	8	4	5	2	2

WORKSHEET 1-1: SELECTION OF PRIMARY THREATS

Worksheet 1-1 will help you to select your primary threats. Building stakeholders and the Assessment Team should review criteria provided in Task 1.3 of this How-To Guide to fill out this Worksheet. After ranking each threat against the provided criteria (Table 1-2), the threat scores should be summed. The top scoring threats (select three to ten of the threats based on score dispersion) become the major threats that you will use for the preparation of your risk assessment.

Criteria								Score
Scenario	**Access to Agent**	**Knowlege/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Level of Defense**	
Improvised Explosive Device (Bomb)								
1-lb. Mail Bomb								
5-lb. Pipe Bomb								
50-lb. Satchel Bomb/ Suicide Bomber								
500-lb. Car Bomb								
5,000-lb. Truck Bomb								
20,000-lb. Truck Bomb								
Natural Gas								

WORKSHEET 1-1: SELECTION OF PRIMARY THREATS (CONTINUED)

Criteria									Score
Scenario		Access to Agent	Knowlege/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense	
Bomb/Aircraft/Ship									
Small Aircraft									
Medium Aircraft									
Large Aircraft									
Ship									
Chemical Agent									
Choking	Chlorine								
	Phosgene								
Blood	Hydrogen Cyanide								
Blister	Lewisite								
Nerve	Sarin								
Biological Agent									
Bacteria	Anthrax								
	Plague								
	Tularemia								
Viruses	Hemorrehagic Fevers								
	Smallpox								
Toxins	Botulinum								
	Ricin								

WORKSHEET 1-1: SELECTION OF PRIMARY THREATS (CONTINUED)

Criteria								Score
Scenario	**Access to Agent**	**Knowlege/ Expertise**	**History of Threats (Building Functions/ Tenants)**	**Asset Visibility/ Symbolic**	**Asset Accessibility**	**Site Population/ Capacity**	**Level of Defense**	
Radiological Agent								
"Dirty Bomb"								
Spent Fuel Storage								
Nuclear Plant								
Armed Attack								
RPG/LAW/Mortar								
Ballistic								
Cyber Attack								
Worm								
Virus								
Denial of Service								

WORKSHEET 1-2: THREAT RATING

Function	Threat Rating (one column for each threat)	Infrastructure	Threat Rating (one column for each threat)
Administration		Site	
Engineering		Architectural	
Warehousing		Structural Systems	
Data Center		Envelope Systems	
Food Service		Utility Systems	
Security		Mechanical Systems	
Housekeeping		Plumbing and Gas Systems	
Day Care		Electrical Systems	
Other		Fire Alarm Systems	
Other		IT/Communications Systems	

Worksheet 1-2 can be used to complete your risk assessment and will be used in conjunction with Worksheets 4-1 and 4-2. It can be used to discuss priority threats with building stakeholders and among the members of the Assessment Team. To fill out this table, analyze the impact of a particular threat on the building core functions and building infrastructure components of your building. Use the results of Worksheet 1-1 to assist you in this process. Building core functions and building infrastructure components are defined in Section 2.3 of this How-To Guide.

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

STEP 2: ASSET VALUE ASSESSMENT

OVERVIEW

The second step in the assessment process is to identify the assets of your area, site, and building that may be affected by a threat (see Figure 2-1). Asset value can be defined as a degree of debilitating impact that would be caused by the incapacity or destruction of an asset. An asset refers to a resource of value requiring protection. It can be tangible (i.e., buildings, facilities, equipment activities, operations, and information) or intangible (i.e., processes or a company's information and reputation).

The asset value assessment process involves the following tasks:

- Identifying the layers of defense
- Identifying the critical assets
- Identifying the building core functions and infrastructure
- Determining the asset value rating

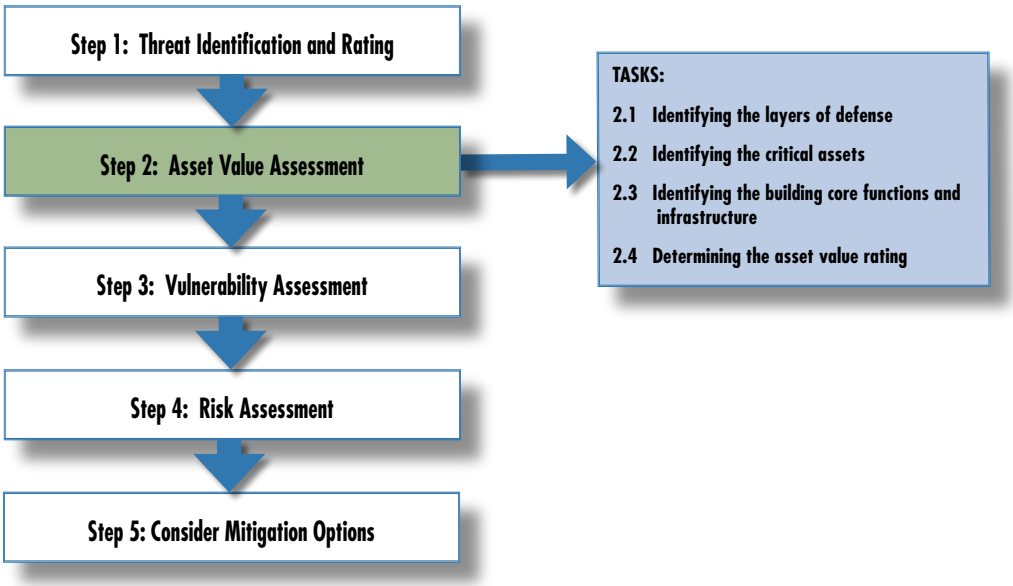


Figure 2-1 Steps and tasks

In this How-To Guide, the identification of the assets is done within the concept of layers of defense. The objective of layers of defense is to create a succeeding number of security layers more difficult to penetrate, provide additional warning and response time, and allow building occupants to move

into defensive positions or designated safe haven protection. This approach will be especially helpful for identifying your mitigation options after you conclude your risk assessment.

To identify and prioritize a building's critical assets is a vital step in the process to improve its level of protection prior to a terrorist attack. Recognizing that people are a building's most critical asset, the process described throughout this step will help you to identify and prioritize those assets where people are most at risk and require protection.

Identifying the Layers of Defense (Task 2.1)

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.

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.

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).

Designers should consider providing adequate stand-off distance when possible. In this case, the hardening of the building is a second choice.

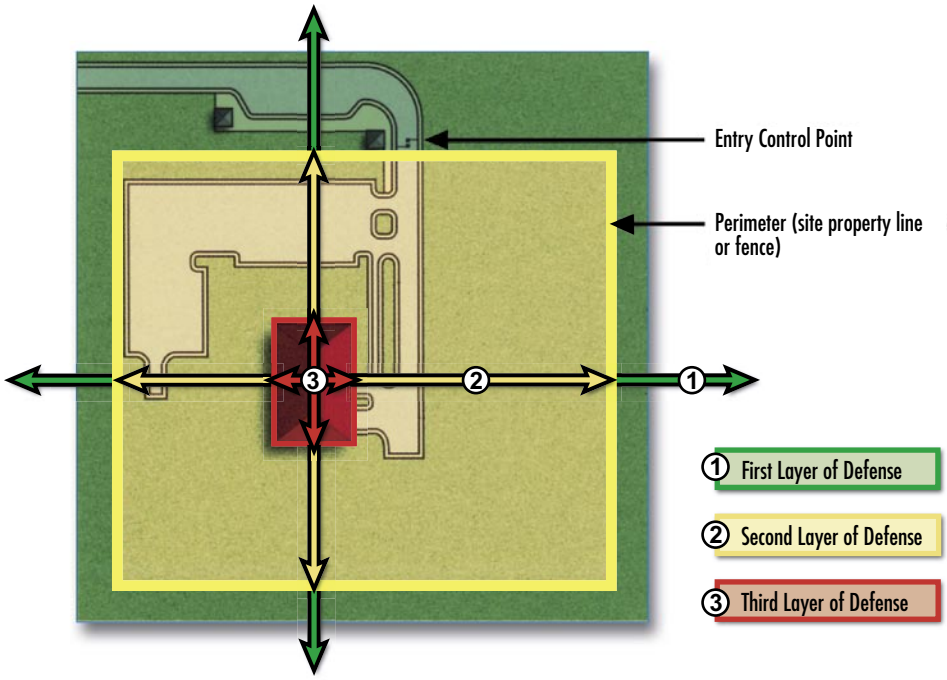


Figure 2-2 Layers of defense

Urban versus Rural

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.

Figure 2-3 depicts the security elements that may be considered in an urban setting. It shows how the second layer of defense becomes extremely important to protect a building in an urban area. Note that the elements described below may require a different method of protection for a campus or a rural site. Major layers for an urban setting include:

- **Curb Lane (First Layer of Defense).** This area refers to the lane of the

street closest to the sidewalk. Typically it is used for curbside parking, passenger drop-off, loading, and service vehicles. Curbside parking should not be removed unless additional stand-off distance is absolutely required for high-target buildings. When required, sidewalks can be widened to incorporate the area devoted to the curb lane.

- **Sidewalk (First Layer of Defense).** This area serves as the common space for pedestrian interaction, moment, and activity. If possible, sidewalks should be left open and accessible to pedestrians and security elements should not interfere with the circulation. The streetscape could include hardened versions of parking meters, streetlights, benches, planters, and trash receptacles. The use of retractable bollards is a great solution when the width of the street does not allow the placement of security elements.

- **Building Yard (Second Layer of Defense).** This area refers to the exterior space between the building and the sidewalk. It consists of a grassy area adjacent to the building flush with the sidewalk or a planted bed raised above the level of the sidewalk. It also includes pedestrian entries and loading docks. For the building yard, security components should complement the building architecture and landscaping. Security elements should be located near the outer edge of the yard. A planter or raised plinth wall provides a good security barrier in this layer.

Figure 2-4 shows the layers of defense in a campus or rural/semi-rural setting that may be required for a campus when a particular building is considered a critical asset. Protection entails considering access points, parking, roadways, pedestrian walkways, natural and physical barriers, security lighting, and signage. Similar situations can be encountered in a campus setting or in a rural or semi-rural area.

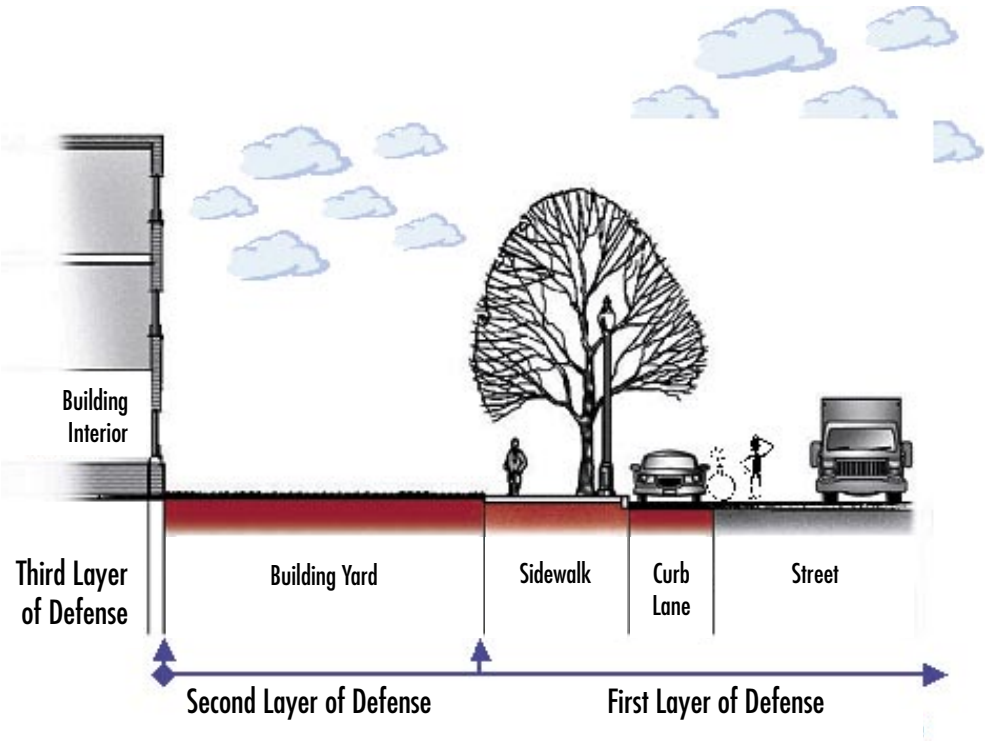


Figure 2-3 Layers of defense in a urban setting

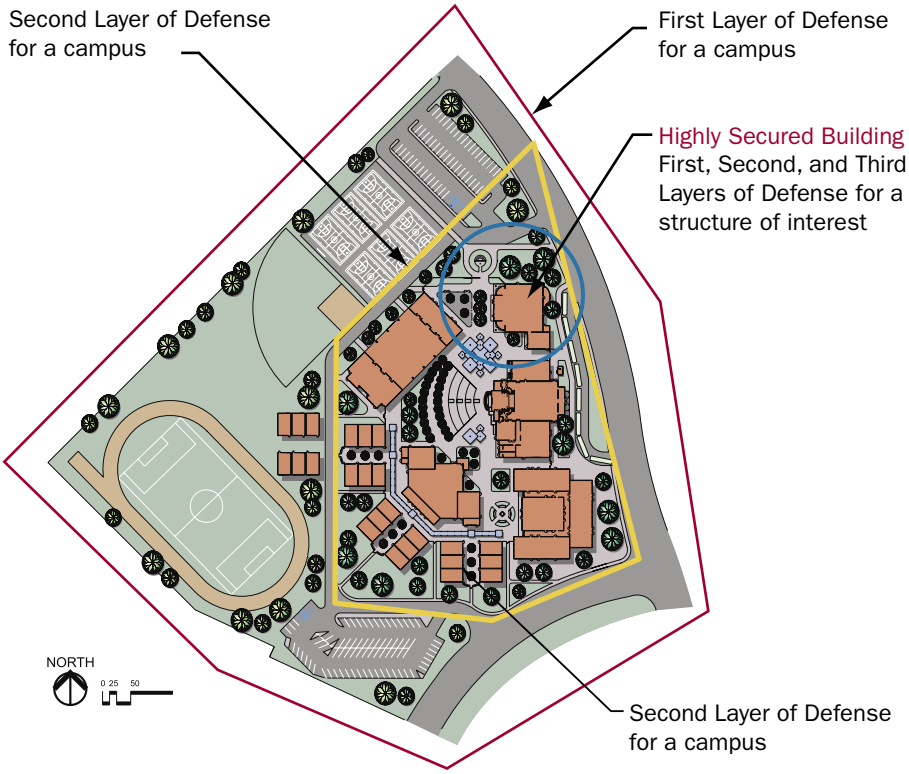


Figure 2-4 Layers of defense when a particular building is considered a critical asset

Identifying the Critical Assets (Task 2.2)

This task involves identifying critical assets within the layers of defense described in Task 2.1. The purpose is to help you determine those assets essential to the minimum operation of your building, and to ensure the health and safety of the building and its occupants. Table 2-1 is a starting point for this exercise. Appendix A of this How-To Guide – the Building Vulnerability Assessment Checklist – provides detailed information regarding the vulnerability of your assets.

Identifying Critical Assets for the First Layer of Defense. One of the first steps when identifying your critical assets is to understand your surrounding areas and how construction types, occupancies, functions, and activities adjacent to your asset can pose a threat or serve to protect your asset. It is essential to understand the interdependencies and distance that separate your building and off-site facilities. Off-site facilities can include:

- Landmarks and iconic buildings
- Law enforcement, fire departments, and hospital buildings
- Federal facilities
- Embassies
- Key commercial properties
- HazMat storage areas and chemical manufacturing plants
- Transportation (roads, avenues of approach, bridges, railroads, tunnels, airports, and ports)
- Telecommunications and utility services

To assess your assets, you may want to consider different scenarios. For example, a car bomb may be able to carry 200 pounds of TNT and a truck bomb may be able to carry 11,000 pounds of TNT. If it is possible that these bombs could be placed proximate to your building, you may want to determine potential damages that they could cause, as well as protective actions for your building. To assess potential damage, the use of Geographic Information Systems (GISs) can be an invaluable resource. Figures 2-5 and 2-6 depict this process. There are several powerful GIS systems available that can help you to

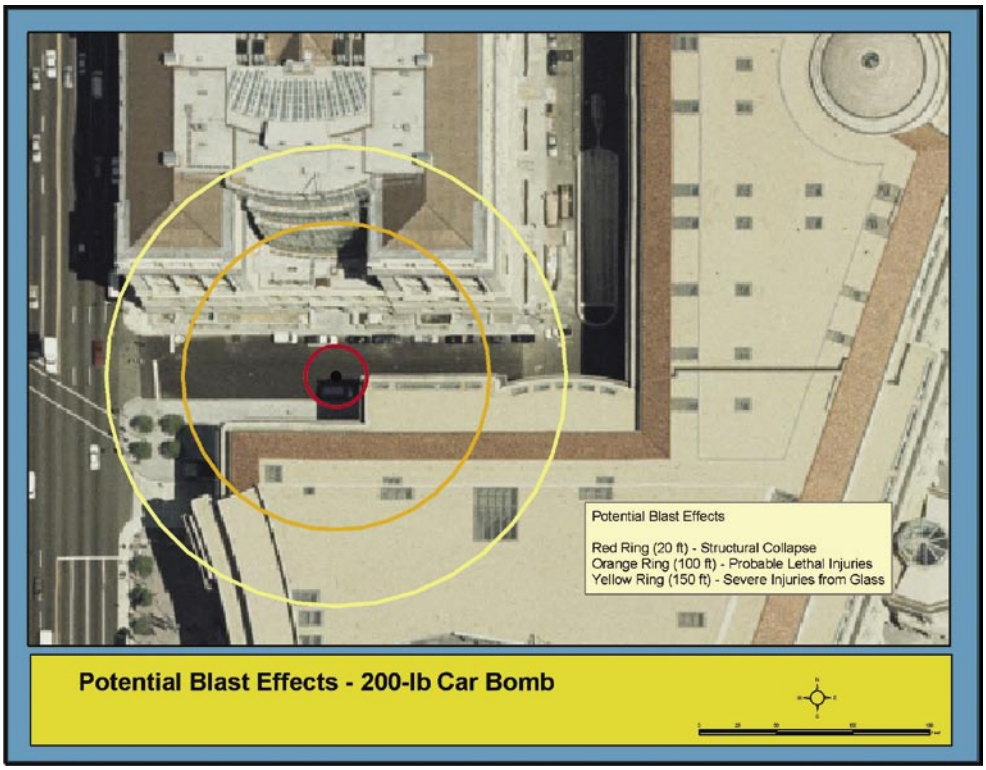


Figure 2-5 Potential blast effects – 200-lb car bomb

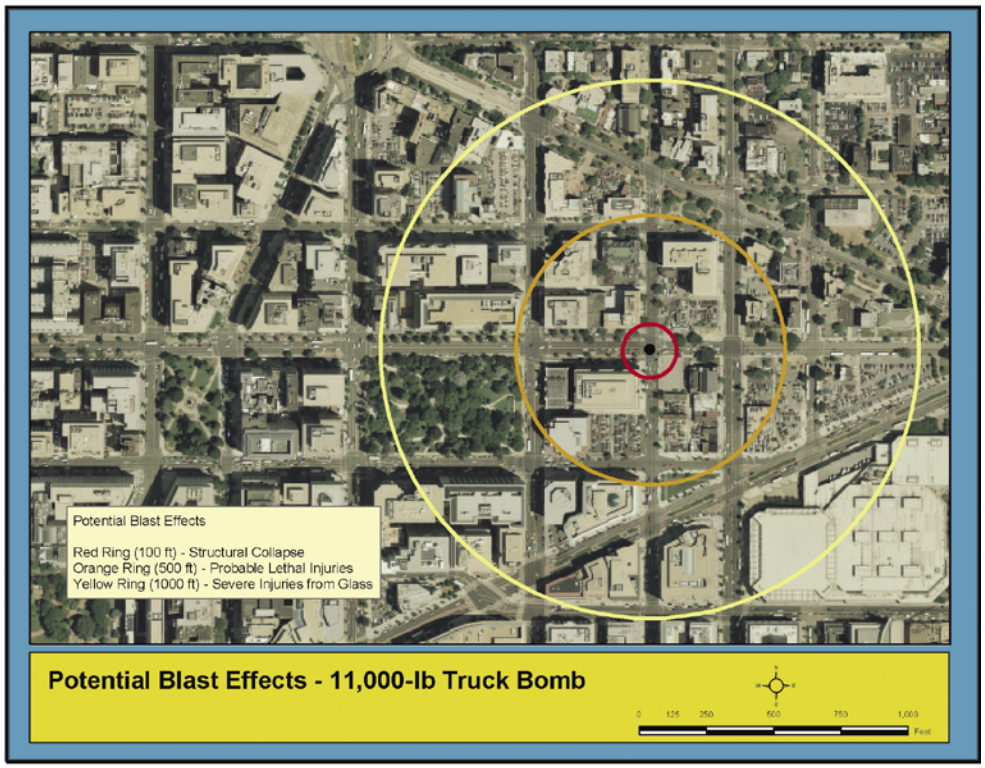
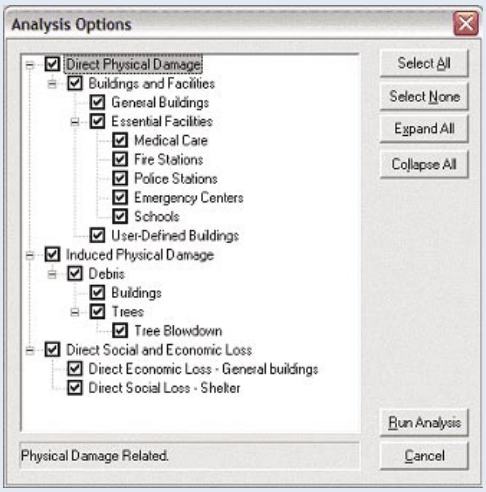


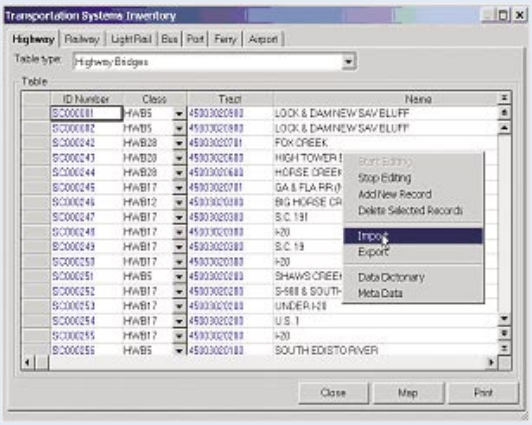
Figure 2-6 Potential blast effects – 11,000-lb truck bomb

HAZUS-MH is a GIS based software developed to estimate losses from earthquakes, floods, and hurricane winds.



HAZUS-MH takes into account various impacts of a hazard event such as:

- Physical damage: damage to residential and commercial buildings, schools, critical facilities, and infrastructure
- Economic loss: lost jobs, business interruptions, and repair and reconstruction costs
- Social impacts: impacts to people, including requirements for shelters and medical aid



HAZUS-MH includes the largest compilation of geo-reference data made available by the Federal Government at no cost. The HAZUS-MH provided inventory data are gathered from the nationally available data sources and include the following:

General Building Stock includes residential, commercial, and industrial building types. HAZUS-MH groups the general building stock into 39 specific model building types and 33 specific occupancy classes.

Essential Facilities include hospitals and other medical facilities, police and fire stations, EOCs, and schools that are often used as shelters.

Hazardous Material Facilities include storage facilities for industrial or hazardous materials such as corrosives, explosives, flammable materials, radioactive materials, and toxins.

High Potential Loss Facilities include nuclear power plants, dams, levees, and military installations.

Figure 2-7 Using HAZUS-MH to identify the criticality of assets

Transportation Lifeline Systems include the following types of infrastructure inventory data:

- Airways – airport facilities, airport runways, heliport facilities, and heliport landing pads
- Highways – bridges, tunnels, and road segments
- Railways – tracks, tunnels, bridges, and facilities (railyards and depots)
- Waterways – ports (locks, seaports, harbors, dry docks, and piers) and ferries
- Bus Stations

Utility Lifeline Systems include potable water, wastewater, oil, natural gas, electric power, and communications systems.

Demographics include people assets of the inventory data regarding total population; age, gender, and race distribution; income distribution; number of owners and renters; building age; and other data obtained from the U.S. Census Bureau and Dun & Bradstreet. The demographic data are aggregated at the Census block or Census tract level.

The database sets in HAZUS-MH are easily converted into visual charts, maps, and graphics for a given site or building.

Training is necessary to run HAZUS-MH and other GIS software. In case of HAZUS-MH, the user must be familiarized with Windows-based environments, GIS software (ArcGIS® 8.3), and data manipulation.

HAZUS-MH is a non-proprietary software that can be ordered at no charge at http://www.fema.gov/hazus

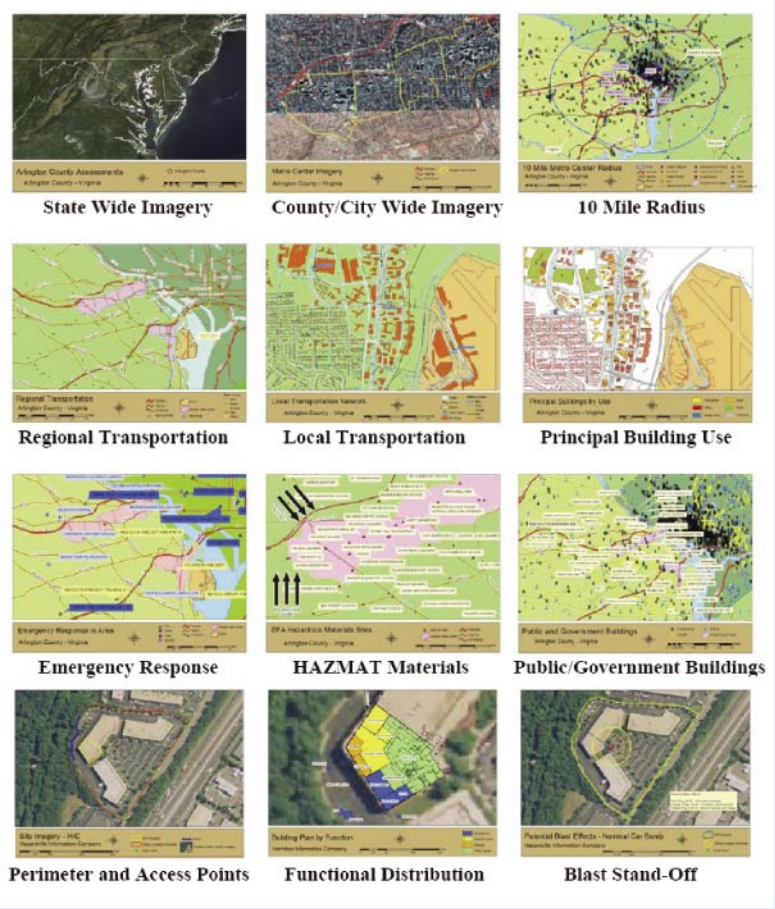


Figure 2-7 Using HAZUS-MH to identify the criticality of assets (continued)

determine your critical asset within the first layer of defense. For this How-To Guide, we suggest the use of HAZUS-MH, described in Figure 2-7. Note that the use of GIS is not required to prepare assessment studies; it is only a tool to facilitate the process.

Identifying Critical Assets for the Second Layer of Defense. To identify your critical assets, you need to understand how important they are in terms of protecting people and key operations. Table 2-1 provides a nominal example of the components that may be of concern when establishing your critical asset. The elements across the top include the different threats that you may have identified. The column to the left provides a list of concerns related to your site. This process can be further expanded by consulting the Building Vulnerability Assessment Checklist in Appendix A. When determining your asset value, you may ask the following questions:

- Are perimeter fences or other types of barrier controls in place?
- What are the access points to the site or building?
- Is there vehicle and pedestrian access control at the perimeter of the site?
- Does site circulation prevent high-speed approaches by vehicles?
- Is there a minimum setback distance between the building and parked vehicles?
- In dense, urban areas, does curb lane parking allow uncontrolled vehicles to park unacceptably close to a building in public rights-of-way?
- What are the existing types of vehicle anti-ram devices for the site or building?
- Do existing landscape measures/features (walls, fountains, berms, etc.) deflect or dissipate the blast pressure?
- Are these devices at the property boundary or at the building?

Identifying Critical Assets for the Third Layer of Defense. When estimating your critical assets within the third layer of defense, you need to consider the structural and non-structural soundness of your building, as well as the possibility of mechanical, plumbing, and electrical systems continuing operations after an attack. Given the evolving nature of the terrorist threat, it is

hard to estimate the value of your assets. For example, due to the catastrophic consequences of progressive collapse, evaluating the structural components of your building can become a high priority. Windows that are the weakest part of a building can become a crucial issue. Other important elements for blast design may include hardening of mechanical and electrical systems and creating appropriate redundancies. The location of air-intakes and limiting the access of the public to main systems can become critical for reducing potential damage from terrorist attacks. The upgrade of HVAC systems and the adoptions of efficient filtering systems can become a key consideration when establishing critical assets.

Table 2-1 is provided to assist you in assessing your critical assets. As previously stated, you may also want to consult the Building Vulnerability Assessment Checklist provided in Appendix A to further analyze your concerns. When determining your critical assets for the third layer of defense, you may ask the following questions:

- What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?
- 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 non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?
- Is the incoming water supply in a secure location? Is there a secure alternate drinking water supply?
- Are the incoming air intakes in a secure location?
- 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?
- Is roof access limited to authorized personnel by means of locking mechanisms?
- What are the types and level of air filtration?
- Are there provisions for air monitors or sensors for CBR agents?

Table 2-1: Correlation of the Layers of Defense Against Threats

■ The symbols indicate which debilitating conditions shown in the left hand column apply to the types of threats indicated across the top of the chart.

	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)	Others
FIRST LAYER OF DEFENSE						
Effects of off-property development have not been considered		■	■	■	■	
Site is within view of other occupied facilities		■				
Site is adjacent to high terrain or structures				■		
Site is close to adjacent dense vegetation			■			
Site is not within low-lying topographic areas				■		
Lack of fencing and physical barriers		■	■	■	■	
Lack of active monitoring for fences and entry points		■	■	■	■	
Insecure access roads to the site		■		■	■	
Lack of entry control and vehicular access		■	■	■	■	
Lack of pull-over lanes at checkpoints to inspect vehicles		■				
Ineffective straight-line vehicular access to high-risk resources		■				
Insecure straight-line entry approach roads		■				
Lack of distance from sidewalk to building yard		■				
SECOND LAYER OF DEFENSE						
Lack of distance from perimeter fence and developed areas		■		■	■	
High-risk resources are not away from primary roads		■		■		
High-risk land uses are not considered in the interior of the site		■				
Lack of sufficient stand-off		■				
Lack of exclusive zone/non-exclusive zones		■				
Facilities with similar threat levels have not been clustered		■		■		
Controlled access zones have not been established		■	■	■	■	
Site critical facilities have not been set on higher ground		■		■		
High surrounding terrain for protected area has not been established		■				
Lack of earth berms used for protection or barriers		■				
Lack of bodies of water used for protection or barriers		■				
Lack of physical obstruction screens		■	■			
Lack of dense thorn-bearing vegetation			■			

Table 2-1: Correlation of the Layers of Defense Against Threats (continued)

	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)	Others
SECOND LAYER OF DEFENSE (continued)						
Lack of vegetation screens			■	■		
Lack of landscape planting to conceal aboveground systems		■	■			
Areas that provide unwanted concealment exist			■	■	■	
Unwanted surveillance is possible		■	■	■	■	
Lack of clear zone for surveillance		■	■	■	■	
Parking surveillance or viewing does not exist		■	■	■	■	
Parking is allowed near high-risk areas		■	■	■	■	
Parking is allowed in exclusive zone		■	■	■	■	
One-way circulation exists		■				
Vehicular access to high-risk resources is not limited		■		■		
Lack of complexes to enhance surveillance opportunities		■	■			
Lack of building yard to place security barriers		■				
Extremely narrow sidewalks that do not permit introducing security elements		■				
Lack of active barriers		■				
Lack of passive barriers		■				
Lack of bollards		■				
Anti-ram street furniture is not in use		■				
Lack of protection in curbs and sidewalks		■				
Lack of enhanced protection close to building entrances		■				
Lack of physical security lighting		■	■	■	■	
Lack of discrete directional signs for high-risk buildings		■	■	■	■	
Lack of major routing corridors away from high-risk resources		■	■	■	■	
High-risk resources are not located far from vehicle parking		■	■	■	■	
Lack of appropriate stand-off zones		■	■			
Lack of separation between facilities		■	■	■		
Lack of separate service and delivery access		■		■	■	
Lack of appropriate location of trash receptacles		■	■	■	■	

Table 2-1: Correlation of the Layers of Defense Against Threats (continued)

	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)	Others
SECOND LAYER OF DEFENSE (continued)						
Vehicle access and closeness to facilities exists		■	■	■	■	
Lack of protection at culverts, sewers, and pipelines			■			
Inappropriate location of loading/unloading docks		■				
Lack of protection at concrete trenches, storm drains, and duct systems			■	■	■	
Lack of check locks on manhole covers			■	■	■	
Inappropriate signs identifying utility systems			■	■	■	
Lack of fencing at critical utility complexes		■	■	■	■	
Lack of appropriate location for fuel/lube storage away from facilities		■	■			
Poor building approach in terms of avenues or streets		■	■			
THIRD LAYER OF DEFENSE						
Inappropriate building configuration		■	■	■	■	
Inappropriate design of lobbies/foyers in terms of concealment versus access		■	■	■	■	
Lack of coded devices	■		■	■	■	
Inappropriate access to public places			■	■	■	
Inappropriate access to private places			■	■	■	
Inappropriate design of public stairwells			■	■	■	
Inappropriate design of private stairwells			■	■	■	
Inappropriate egress/ingress			■	■	■	
Unreinforced envelope systems		■	■			
Weak bearing walls		■	■			
Weak non-bearing walls		■	■			
Inappropriate design/level of fenestration		■	■			
Unreinforced windows		■	■			
Unreinforced window frames		■	■			
Unreinforced mullions		■	■			
Inappropriate glass design		■	■			
Unreinforced doors		■	■	■	■	

Table 2-1: Correlation of the Layers of Defense Against Threats (continued)

	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)	Others
THIRD LAYER OF DEFENSE (continued)						
Unreinforced door frames		■	■	■	■	
Inappropriate window frame and anchorage design		■	■			
Inappropriate access to roof			■	■	■	
Lack of blast-resistant roof		■				
Inappropriate location of mail room				■	■	
Inappropriate data center location/protection		■	■	■	■	
Underground garages		■	■			
Inappropriate location of public restrooms			■	■	■	
Inappropriate design of loading docks		■	■			
Lack of shelter-in-place		■		■	■	
Lack of security lighting		■	■	■	■	
Lack of progressive collapse considerations		■	■			
Inappropriate column spacing/redundancy		■	■			
Lack of ductile structural elements and detailing		■	■			
Inappropriate sheer reinforcement		■	■			
Lack of symmetric steel reinforcement		■	■			
Lack of appropriate steel connections/moment connections		■	■			
Lack of lateral and vertical force redundancy systems		■	■			
Inadequate redundant load paths		■	■			
Inadequate transfer girders		■	■			
Inadequate grouting and reinforcement of masonry		■	■			
Lack of reinforcement of non-bearing masonry walls		■	■			
Lack of CBR/mechanical considerations	■		■	■	■	
Lack of air supply/return duct connections			■	■	■	
HVAC control centers/redundant equipment	■		■	■	■	
HVAC/filtration				■	■	
Lack of HVAC control wiring/routing	■			■	■	

Table 2-1: Correlation of the Layers of Defense and Threats (continued)

	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)	Others
THIRD LAYER OF DEFENSE (continued)						
Lack of HVAC purge capacity				■	■	
Easy access to plumbing system				■	■	
Poor method gas distribution/entry points				■	■	
Inappropriate central shaft				■	■	
Inappropriate main piping distribution				■	■	
Inappropriate gas storage tanks		■	■			
Inappropriate gas reserve supplies location		■	■			
Inappropriate electrical rooms/location/protection		■	■			
Inappropriate primary electrical wiring location/protection		■	■			
Inappropriate transformers/location/protection		■	■			
Inappropriate switchgears/location/protection		■	■			
Inappropriate distribution panels location/protection		■	■			
Inappropriate branch circuits/location/protection		■	■			
Lack of backup power/distribution		■	■			
Inappropriate fire protection		■	■			
Inappropriate fire alarm panels/location/protection		■	■			
Lack of fire alarm system/blast-resistant		■	■			
Lack of off-site redundant systems for fire alarm reporting	■	■	■			
Inappropriate fire hydrant location		■	■			
Inappropriate smoke evacuation systems		■	■	■	■	
Inappropriate communications/surveillance systems	■	■	■	■	■	
Inappropriate telephone distribution room /location/protection	■	■	■			
Lack of non-interruptible power supply	■	■	■			
Inappropriate communications system wiring closets location/protection	■	■	■			
Inappropriate communications wiring distribution	■	■	■			
Lack of redundancy	■	■	■			
Lack of secondary/intermediary distribution facilities	■	■				

Table 2-1: Correlation of the Layers of Defense Against Threats (continued)

	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)	Others
THIRD LAYER OF DEFENSE (continued)						
Minimum points of presence		■	■	■	■	
Ineffective WAN systems	■					
Ineffective LAN systems	■					
Ineffective radio/wireless systems/location/protection	■		■			
Ineffective CCTV/location/protection	■		■	■	■	

Identifying the Building Core Functions and Infrastructure (Task 2.3)

The identification of the building core functions and infrastructure is one of the key elements of the assessment. These functions are the basis for the analysis described in this How-To Guide. The functions and infrastructure analyses identify the geographic distribution within the building and interdependencies between critical assets. Ideally, the functions should have geographic dispersion as well as a pre-determined recovery site or alternate work location. Similarly, critical infrastructure should have geographic dispersion and backup. For example, a bomb or CBR attack entering through the loading dock could impact the telecommunications, data, uninterruptible power supply (UPS), generator, and other key infrastructure systems. The core functions and infrastructure are described below.

Identifying Building Core Functions

The first activity is to determine the core functions and processes necessary for the building to continue to operate or provide services after an attack. The reason for identifying core functions/processes is to focus the Assessment Team on what a building does, how it does it, and how various threats can affect the building. This provides more discussion and results in a better understanding of asset value. Factors that should be considered include:

- What are the building's primary services or outputs?

- What critical activities take place at the building?
- Who are the building's occupants and visitors?
- What inputs from external organizations are required for a building's success?

A number of core functions have been selected for this How-To Guide and are included in Table 2-2.

Table 2-2: Building Core Functions

Building Core Functions
Administration
Engineering
Warehousing
Data Center
Food Service
Security
Housekeeping
Day Care

Identifying Building Core Infrastructure

After the core functions and processes are identified, an evaluation of building infrastructure should follow. To help identify and value rank infrastructure, the following should be considered, keeping in mind that the most vital asset for every building is its people:

- Identify how many people may be injured or killed during a terrorist attack that directly affects the infrastructure.
- Identify what happens to occupants if a specific asset is lost or degraded. (Can primary services continue?)
- Determine the impact on other organizational assets if the component is lost or can not function.
- Determine if critical or sensitive information is stored or handled at the building.

- ❍ Determine if backups exist for the building's assets.
- ❍ Determine the availability of replacements.
- ❍ Determine the potential for injuries or deaths from any catastrophic event at the building's assets.
- ❍ Identify any critical building personnel whose loss would degrade or seriously complicate the safety of building occupants during an emergency.
- ❍ Determine if the building's assets can be replaced and identify replacement costs if the building is lost.
- ❍ Identify the locations of key equipment and the impact if it is lost during a terrorist attack.
- ❍ Determine the locations of personnel work areas and systems.
- ❍ Identify the locations of any personnel operating "outside" a building's controlled areas.
- ❍ Determine, in detail, the physical locations of critical support architectures:
    - Communications and information technology (i.e., the flow of critical information)
    - Utilities (e.g., facility power, water, air conditioning, etc.)
    - Lines of communication that provide access to external resources and provide movement of people (e.g., road, rail, air transportation)
- ❍ Determine the location, availability, and readiness condition of emergency response assets, and the state of training of building staff in their use.

A number of core infrastructures have been selected for this How-To Guide. Table 2-3 includes the selected examples.

Table 2-3: Building Core Infrastructure

Building Core Infrastructure
Site
Architectural
Structural Systems
Envelope Systems
Utility Systems
Mechanical Systems
Plumbing and Gas Systems
Electrical Systems
Fire Alarm Systems
IT/Communications Systems

Levels of Protection

The selection of the level of protection is building-dependent. The General Services Administration (GSA) and DoD have developed standards and recommendations that can be applicable to buildings leased by or used to support Federal Government agencies. These standards and recommendations are not required for non-Federal buildings; however, building owners can evaluate and select those standards that meet their specific needs and criteria.

A primary concern is the protection of buildings from explosive blast and CBR attacks. To protect against blast, the level of protection is dependent upon the type of construction and the blast pressures (stand-off distance). The amount of explosive and the resulting blast dictate the level of protection required to prevent a building from collapsing or minimizing injuries and deaths. Levels of protection can be found in GSA PBS-P100, *Facilities Standards for the Public Buildings Service,* November 2000, Section 8.6 and USAF *Installation Force Protection Guide* and DoD UFC-010-01.

The DoD prescribes minimum stand-off distances based on the required level of protection. Where minimum stand-off distances are met, conventional construction techniques can be used with some modifications. In cases where the minimum stand-off cannot be achieved, the building must be hardened to achieve the required level of protection. The DHS and Interagency Security Committee (ISC) Security Criteria (GSA was formerly responsible for this In-

teragency Committee) do not require or mandate specific stand-off distances. Rather, they provide protection performance criteria. In order to economically meet these performance standards, they present recommended stand-off distances for vehicles that are parked on adjacent properties and for vehicles that are parked on the building site (see GSA *Security Criteria,* Draft Revision, October 8, 1997, and ISC *Security Design Criteria for New Federal Office Buildings and Major Modernization Projects,* May 28, 2001). Table 2-4 presents the levels of protection and the recommended security measures.

Table 2-4: Levels of Protection and Recommended Security Measures*

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 with 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 with Closed Circuit Television (CCTV) Visitor Control/Screening Shipping/Receiving Procedures Guard/Patrol Assessment Intrusion Detection with Central Monitoring CCTV Surveillance (Pan-Tilt, Zoom System) Duress Alarm with Central Monitoring

Table 2-4: Levels of Protection and Recommended Security Measures* (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 Offices Local Schools Commercial Facilities Industrial Manufacturing Health Care	Guard Patrol on Site Visitor Control/Screening Shipping/Receiving Procedures Intrusion Detection with Central Monitoring CCTV Surveillance (Pan-Tilt, Zoom System) Duress Alarm with 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

** Source: U.S. Department of Justice, Vulnerability Assessment of Federal Facilities, June 28, 1995*

*NOTES: ** Assignment of levels to be based on an "on-site" risk assessment/evaluation*

****Examples of typical (but not limited to) tenant agencies for this level facility*

Establishing the levels of protection for CBR agents is more difficult to quantify because there are almost infinite agents and delivery modes that can be used and a CBR attack affects multiple systems. Protection against CBR attacks is focused on preventing agents from entering a building and using the building envelope and HVAC system to respond to an attack to isolate or contain an agent to as small a footprint as possible.

For more information on explosive blast and CBR, you may consult DoD and GSA standards; the Building Vulnerability Assessment Checklist in Appendix A; FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings;* FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks;* and the CDC guides for protection against CBR attack and filtration.

Determining the Asset Value Rating (Task 2.4)

After building core functions and building infrastructure are analyzed, a value should be assigned. Table 2-5 provides a scale for selecting your asset value. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). To determine a value, you should keep in mind that asset value can be defined as the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets. To determine a vulnerability rating, you should consider the consequences of the loss or damage of the building's assets (e.g., loss of life, injuries, or total loss of primary services, core processes and functions). The key asset for every building is its people (e.g., employees, visitors, etc.) and they will always be assigned the highest asset value. Tables 2-6A and 2-6B display a nominal example applying these ratings for an urban multi-story building.

Table 2-5: Asset Value Scale

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 of 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.
Medium	5-6	Medium – Loss or damage of the building's assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes.
Medium Low	4	Medium Low – Loss or damage of the building's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes.
Low	2-3	Low – Loss or damage of the building's assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.
Very Low	1	Very Low – Loss or damage of the building's assets would have negligible consequences or impact.

Table 2-6A: Nominal Example of Asset Value Rating for an Urban Multi-story Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	5	5	5	5	5
Engineering	8	8	8	8	8
Warehousing	3	3	3	3	3
Data Center	8	8	8	8	8
Food Service	2	2	2	2	2
Security	7	7	7	7	7
Housekeeping	2	2	2	2	2
Day Care	10	10	10	10	10

Table 2-6B: Nominal Example of Asset Value Rating for an Urban Multi-story Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	4	4	4	4	4
Architectural	5	5	5	5	5
Structural Systems	8	8	8	8	8
Envelope Systems	7	7	7	7	7
Utility Systems	7	7	7	7	7
Mechanical Systems	7	7	7	7	7
Plumbing and Gas Systems	5	5	5	5	5
Electrical Systems	7	7	7	7	7
Fire Alarm Systems	9	9	9	9	9
IT/Communications Systems	8	8	8	8	8

The following additional references for blast are recommended:

U.S. Air Force, 1989, ESL-TR-87-57, *Protective Construction Design Manual*, **Contact Airbus Technologies Division (AFRL/MLQ) at Tyndall Air Force Base, Florida, via e-mail to techinfo@afrl.af.mil. [Superseded by Army Technical Manual TM 5-855-1 (Air Force Pamphlet AFPAM 32-1147(I), Navy Manual NAVFAC P-1080, DSWA Manual DAHSCWEMAN-97), December 1997]**

U.S. Army Corps of Engineers, 1990, TM 5-1300, *Structures to Resist Accidental Explosions*, **U.S. Army Corps of Engineers, Washington, D.C., (also Navy NAVFAC (Naval Facilities) P-397, Air Force Regulation 88-2); Contact David Hyde, U.S. Army Engineer Research and Development Center, 3909 Halls Ferry Road, Vicksburg, Mississippi 39180 or via e-mail to hyded@ex1.wes.army.mil**

U.S. Department of Energy, 1992, DOE/TIC 11268, *A Manual for the Prediction of Blast and Fragment Loadings on Structures*, **Southwest Research Institute, Albuquerque, New Mexico.**

Technical Support Working Group, Terrorist Bomb Threat Stand-Off Card with Explanation of Use, Technical Support Working Group, Washington, D.C. http://www.tswg.gov/tswg/prods_pubs/newBTSCPress.htm

U.S. Department of the Treasury/Bureau of Alcohol, Tobacco and Firearms, 1999, Vehicle Bomb Explosion Hazard And Evacuation Distance Tables, Department of the Treasury, Washington, D.C. (Request in writing, address information available at http://www.atf.treas.gov/pub/fire-explo_pub/i54001.htm)

Federal Bureau of Investigation, 1999, *Terrorism in the United States.*

Department of Justice, Federal Bureau of Investigation, Counterterrorism Division, Washington, DC. http://www.fbi.gov/publications/terror/terror99.pdf

The U.S. Department of State, 2002, *Patterns of Global Terrorism 2001.*

Biggs, John M. *Introduction to Structural Dynamics.* McGraw-Hill. 1964.

The Institute of Structural Engineers. *The Structural Engineer's Response to Explosive Damage.* SETO, Ltd., 11 Upper Belgrave Street, London SW1X8BH. 1995.

Mays, G.S. and Smith, P.D. *Blast Effects on Buildings: Design of Buildings to Optimize Resistance to Blast Loading.* Thomas Telford Publications, 1 Heron Quay, London E14 4JD. 1995.

National Research Council. *Protecting Buildings from Bomb Damage.* National Academy Press. 1995.

WORKSHEET 2-1: ASSET VALUE

Function	Asset Value	Infrastructure	Asset Value
Administration		Site	
Engineering		Architectural	
Warehousing		Structural Systems	
Data Center		Envelope Systems	
Food Service		Utility Systems	
Security		Mechanical Systems	
Housekeeping		Plumbing and Gas Systems	
Day Care		Electrical Systems	
Other		Fire Alarm Systems	
Other		IT/Communications Systems	

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

Worksheet 2-1 can be used to complete your risk assessment and will be used in conjunction with Worksheets 4-1 and 4-2. It can be used to discuss asset value with building stakeholders and among the members of the Assessment Team. Asset value refers to a resource of value requiring protection. A scale (asset value) can be used to signify the protection that a particular asset merits. To fill out this table, analyze the impact of a particular threat to your site and/or building. Analyze core functions and building infrastructure components as indicated in Task 2.3.

STEP 3: VULNERABILITY ASSESSMENT

OVERVIEW

The third step in the assessment process is to prepare a vulnerability assessment of your assets that can be affected by a threat (see Figure 3-1). For this document, vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to hazard damage. A vulnerability assessment is an indepth 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. During this step, you will begin the analysis of your assets based on: a) the identified threat; b) the criticality of your assets: and c) the level of protection you may have chosen (i.e., your willingness or unwillingness to accept risk).

The vulnerability assessment process involves the following tasks:

- Organizing resources to prepare the assessment
- Evaluating the site and building
- Preparing a vulnerability portfolio
- Determining the vulnerability rating

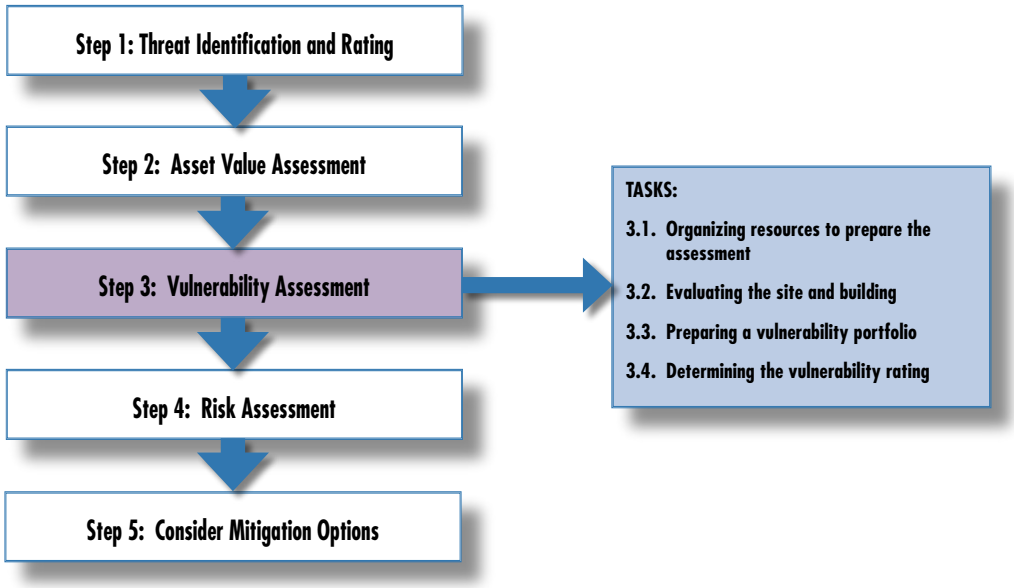


Figure 3-1 Steps and tasks

Organizing Resources to Prepare the Assessment (Task 3.1)

An important task during Step 3 is organizing your resources to prepare the assessment. This involves determining the level of the assessment you wish to perform and the skills of the team necessary to conduct the assessment.

Selecting the Assessment Team

The selection of the Assessment Team is probably the most critical task in the threat assessment process. An assessment has been found to be most effective when the Team is composed of senior individuals who have a breadth and depth of experience and understand other disciplines and system interdependencies. The Assessment Team leader will work with the building owner and stakeholders to:

- Determine the threat rating (Step 1)
- Determine the asset value and level of protection (Step 2)

The Assessment Team will coordinate the preparation of an assessment schedule, assessment agenda, and on-site visit assessments with the building stakeholders. It is important to emphasize that the Assessment Team should be composed of professionals capable of evaluating different parts of the buildings and familiar with engineering, architecture and site planning. Other members of the team may include law-enforcement agents, first responders, and building owners and managers.

Determining the Level of the Assessment

The level of the assessment for a given building is dependent upon a number of factors such as type of building, location, type of construction, number of occupants, economic life, and other owner specific concerns and available economic resources. The levels of the assessment provided in this How-To Guide are similar to the FEMA 310 process and provide increasing tiers of assessments. The underlying purpose is to provide a variable scale to meet benefit/cost considerations for a given building that meets the intent and requirements of available antiterrorism guidelines such as the DoD Minimum Antiterrorism Standards and the GSA Interagency Security Criteria.

Tier 1. A Tier 1 assessment is a 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 ex-

perienced 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 non-critical facilities and infrastructure.

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 indepth 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.

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 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.

Table 3-1: Tier 1 - Screening Phase

Task	Building Type	Team Composition	Duration	Activity
Information Gathering and Review	Standard commercial office building	1 Site and Architectural	1 day	Review technical area and general site analysis
On-site Evaluation		1 Security Systems and Operations	1 day per assessor	• Complete the Critical Function and Critical Infrastructure matrices; perform a limited technical review using the Building Vulnerability Assessment Checklist; input site, vulnerability, and mitigation information into the database; write reports • Prepare a verbal or PowerPoint presentation with key findings to review with building owners' and stakeholders' major findings • Receive input on the assessment process
Develop Mitigation Options			Typically 1 to 3 days per assessor	• Prepare a Preliminary Report, including findings and feedback from stakeholders. This report should include concept and cost mitigation options. • Prepare a written Final Report that lists the vulnerabilities, observations, and mitigation options. Very rough order of magnitude cost estimates may be developed using standard unit costs for blast, CBR, and physical security infrastructure and equipment. • Prepare a Vulnerability Portfolio with recommendations for incorporation into Emergency Operations, Disaster Recovery, and other plans or procedures

Table 3-2: Tier 2 - Full On-site Evaluation

Task	Building Type	Team Composition	Duration	Activity
Information Gathering and Review	High-risk or iconic buildings Commercial buildings, government facilities, schools, and hospitals Designated high asset value infrastructure	1 Site and Architectural (recommended as Team leader) 1 Structural and Building Envelope 1 Mechanical, Electrical, and Power Systems and Site Utilities 1 Landscape Architect 1 IT and Telecommunications 1 Security Systems and Operations	1 day per assessor	Review technical area and general site analysis collected during the Tier 1 assessment
On-Site Evaluation			2 to 4 days per assessor	• Complete the Critical Function and Critical Infrastructure matrices; perform a limited technical review using the Building Vulnerability Assessment Checklist; input site, vulnerability, and mitigation information into the database; write reports • Prepare a verbal or PowerPoint presentation with key findings to review with building owners' and stakeholders' major findings • Receive input on the assessment process
Develop Mitigation Options			1 to 3 days per assessor	• Prepare a Preliminary Report, including findings and feedback from stakeholders. This report should include concept and cost mitigation options. • Prepare a written Final Report that lists the vulnerabilities, observations, and mitigation options. Very rough order of magnitude cost estimates may be developed using standard unit costs for blast, CBR, and physical security infrastructure and equipment. • Prepare a Vulnerability Portfolio with recommendations for incorporation into Emergency Operations, Disaster Recovery, and other plans or procedures

Table 3-3: Tier 3 - Detailed Evaluation

Building Type	Team Composition	Activity
High value and critical infrastructure assets	1 Site and Architectural - Team leader 1 Structural and Building Envelope 1 Mechanical, Electrical, and Power Systems and Site Utilities 1 IT and Telecommunications Modeler 1 Security Systems and Operations 1 Explosive Blast Modeler 1 CBR Modeler 1 Cost Engineer 1 Landscape Architect	• A typical Tier 3 Assessment Team will use the results of the Tier 2 assessment and involve modeling and analysis of the building and related systems using advanced blast and WMD models and applications. Blast analysis will include structural progressive collapse, glazing, and effects of building hardening. CBR analysis should evaluate the effects of the agents released externally and internally to provide the dispersion, duration, and exposure of the building systems and occupants. The IT and Telecommunications Modeler should evaluate effects on all IT systems assuming cascading equipment failure and long-term access denial to critical equipment, data, and on-site administrative capability. • The Tier 3 assessment will provide detailed building response, survivability, and recovery information used to develop enhanced and accurate costing of mitigation options.

Evaluating the Site and Building (Task 3.2)

Understanding the type, nature, and geographic range of threats (Step 1) that can occur at your site or building, as well as the associated exposure of your assets (Step 2) is essential to conducting a vulnerability analysis. Each building, even if on the same campus or the same general area, can have different priority threats and hazards. A well-prepared risk manager must be aware of the types of threat and hazard events that can occur, the areas and resources most at risk, and the potential costs and losses that could accompany a threat or hazard event.

To prepare an effective assessment, the following activities should take place:

1. **Pre-Meeting and Preparation of a Schedule and Tentative Agenda.** Before conducting the on-site building evaluation, a coordination meeting should take place. During this meeting, the type of assessment to be conducted, personnel availability, schedules, and outputs should be discussed in detail. In addition, firm timetables and an agenda for on-site visits should be discussed. The agenda schedule should include the sites to be evaluated and special areas to be protected. Worksheets 3-1 and 3-2 have been developed to aid in this process.

2. **On-Site Meeting(s).** For each assessment, a preparation meeting will take place with key stakeholders. Upon arrival at the site or building, the Team should have an introduction meeting with key staff, review the available information, and review the vulnerability portfolio (Task 3.3). As a minimum, recommended building personnel attendees should include:

   - Site or building owner
   - Chief of engineering
   - Chief of security
   - Chief of IT
   - Emergency manager

Other attendees may include:

- Union or employee representatives
- Local law enforcement, fire, and EMS representatives
- State or county representatives

- Local utility, telecommunications, and services (waste, security services, etc.)
- Administration, food services, laboratory, and other critical function representatives

For the assessment to be successful, building stakeholders should participate as key members, providing on-site access to all buildings and areas. In addition, they should participate in interviews, and provide comments on current strengths and weakness of plans and procedures, including facility access, personnel movement, operations and maintenance, and security alerts.

3. **Windshield Tour(s).** After the introduction meeting, the Assessment Team and stakeholders should conduct a "windshield" tour or walk-around of the key facilities. The Assessment Team may find areas that require special attention and feel the need to make adjustments to the assessment agenda (Worksheet 3-2).

4. **Assessment Background Information.** After the on-site tour, the Assessment Team and stakeholders are ready to conduct the on-site assessment. Completing the matrices provided in this How-To Guide for conducting the threat assessment will take approximately 4 to 8 hours, using an interview and consensus approach around a table. During these discussions, the Team should prepare worksheets provided in Steps 1 and 2. They will determine:

   - Threats that are a priority concern for your site, building, and related infrastructure (Worksheets 1-1 and 1-2)
   - The assets of your area, building or site that can be affected by a threat (Worksheet 2-1)

5. **Review Key Documents.** The Assessment Team will review or evaluate a number of plans, procedures, and policies. The list below provides some of the documents that need to be reviewed by the Team before conducting the assessment. How to gather this information is described in Steps 1 and 2.

   - Prior vulnerability assessment data
   - Emergency response and disaster recovery plans
   - Security master plan (including detection/delay/assess)

- Security inspection results
- HazMat plans
- Policy and legal requirements
- Federal, State, and local law enforcement threat assessments
- Site plans of utility and communications systems
- Floor plans for all facilities identified as important (including those listed above)
- Floor plans and locations of modified and abandoned facilities
- Structural drawings of key facilities
- New project drawings for fences, security, and buildings
- Security system drawings
- Historical reports
- Local zoning ordinances
- Comprehensive plans
- Development plans
- Information on the facility systems operations capability
- Information on agreements with the surrounding community and Federal agencies
- Information on incidents within the building (i.e., misconduct information)
- Population statistics
- Manpower surveys
- Other documents determined by the Team to be important

6. **Review Emergency Procedures.** The Assessment Team and building stakeholders should review the security master plan, and the engineering operations and maintenance, emergency operations, and disaster recovery plans to understand the critical assets of the building and establish a baseline organization response and recovery capability in case of an attack or event. The impact of many vulnerabilities can be reduced or eliminated by simple changes in plans, policies, and procedures.
   As part of the screening phase review, the following areas should be considered:

- Emergency notification procedures
- Emergency evacuation procedures
- First responder access and routing
- Shelter-in-place procedures
- Designated shelter capacities and travel routes
- Off-site rally point and roll call
- Emergency engineering systems shutdown (HVAC, electrical, information technology (IT)/telecommunications)
- Portable protective equipment (indoor air filters, sampling kits, first aid)
- Personal protective equipment (PPE)
- Exercise of plans

7. **Prepare the Assessment.** Preparing the assessment can be as simple as a quick review and analysis of existing documents and a short walk around the site, or a more detailed in-depth review and analysis of the documents, plans, and other information and a thorough walk-through of the building, including utility spaces, basements, crawl spaces, attics, and vault (see Tables 3-1, 3-2, and 3-3). The following are recommended when conducting the different types of assessments.

   For Tier 1 Screening Evaluation, the analysis should include, at a minimum:

   - Perimeter identification
   - Vehicle and pedestrian entry access control points
   - Security operations function
   - EOC (or function)
   - Primary point of entry of utilities and telecommunications
   - Critical functions
   - Critical infrastructure
   - Key staff
   - Off-site rally point and other Emergency Management procedures (PPE, mass notification, etc.)

For Tier 2 On-Site Evaluation, the analysis should include, at a minimum:

- Tier 1 information
- Detailed inspection and route tracing of primary utilities and telecommunications
- Detailed review of HVAC system and operating parameters
- Detailed review of electric power and generator capacity (life safety, data centers, communications, etc.)
- Detailed review of structural and envelope system (column-beam connections, materials, clips, glazing)
- Detailed review of Security Master Plan, Emergency Management Plan, other related plans and Memorandums of Understanding (MOU) (Continuity of Operations [COOP], Continuity of Government [COG], Certified Emergency Management Plan [CEMP], etc.)

For Tier 3, Detailed Evaluation, the analysis should include, at a minimum:

- Tier 2 information
- Systems interdependencies on-site and off-site (utility vaults, communications central office trunks, transportation nodes, logistics, etc.)
- Advanced blast and CBR modeling of building and systems (structural damage, interior and exterior plume dispersion, safe haven areas)
- Advanced evacuation planning and routing to include test of mass notification system, training, and exercises
- Advanced disaster response and recovery planning in conjunction with neighbors and local government

8. **Data Gap Analysis.** The Assessment Team may feel that the data gathered for on-site assessment are not enough. The Team should assess the following information:

   - Do we know where the greatest damages may occur in the threat/hazard areas?
   - Do we know whether critical facilities will be operational after a threat/hazard event?

- Are there enough data to determine which assets are subject to the greatest potential damages?
- Are there enough data to determine whether significant elements of the community are vulnerable to potential threats?
- Are there enough data to determine whether certain areas of historic, environmental, political, or cultural significance are vulnerable to potential threats?
- Is there concern about a particular threat because of its severity, frequency, or likelihood of occurrence?
- Are additional data needed to justify the expenditure of community or state funds for mitigation initiatives?

If the Team decides that more data will be beneficial to conduct the assessment, a determination should be made as to what type of data are needed and what resources are available for collecting new data. If stakeholders and the Team agree on collecting new data, the Team needs to prioritize areas for additional data collection.

Preparing a Vulnerability Portfolio (Task 3.3)

To carry out the assessment, the Team should have a vulnerability portfolio available. This portfolio should include the following:

- ❍ Assessment agenda (Worksheet 3-2)
- ❍ Assessment background information (to be collected by Assessment Team and building owners)
- ❍ Threats rating (Worksheets 1-1 and 1-2)
- ❍ Asset value ranking worksheet (Worksheet 2-1)
- ❍ Key documents (plans, procedures, and policies, see Task 3.2)
- ❍ Emergency procedures (baseline organization response and recovery capability in case of an attack or event, see Task 3.2)
- ❍ Building Vulnerability Assessment Checklist (Appendix A)
- ❍ Risk assessment matrices (Worksheets 4-1 and 4-2, described in Step 4)

- Prioritization of observations in the checklist (Worksheet 4-3)

- Risk Assessment Database (if assessment is going to be automated – see Appendix B)

The Building Vulnerability Assessment Checklist, the Pre-Assessment Screening Matrix, and the Risk Assessment Database are explained below.

Building Vulnerability Assessment Checklist. Appendix A includes the Building Vulnerability Assessment Checklist, 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. It allows a consistent security evaluation of designs at various levels.

The Checklist is a key tool in the preparation of the threat assessment and a fundamental element of your vulnerability portfolio. When performing a walk-through of the facility to be assessed, the Team should use the Checklist as a screening tool for preparing the vulnerability assessment and make observations when reviewing the questions included in the Checklist.

The Checklist is organized into 13 sections. To conduct a vulnerability assessment of a building or preliminary design, each section of the Checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area. Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. The observations made during this Step will be prioritized during Step 4. The observations in the Checklist should be supplemented with photographs, if possible.

Risk Assessment Database. To support the building assessment process, a simple and easy to use Risk Assessment Database application is provided with this manual (see Appendix B). This database was originally developed for the Department of Veterans Affairs (VA) through the National Institute of Building Sciences (NIBS). It has already been used in the assessment of over 100 hospitals, office buildings, data centers, and other facilities across the United States. FEMA modified this database in order to make it easy-to-use for commercial buildings. The database is a stand-alone application that has functions, folders to import and display digital photos, emergency plans, digital floor plans, and certain HAZUS-MH products. Information retrieved from HAZUS-MH and existing commercial off the shelf (COTS) software such as Facility Condition Assessment, Work Order, Real Estate, and Space and

Planning applications can be used in conjunction with the database for the assessment. Site, Team, and other general information is collected and inputted using screens. This database contains the basic information included in the Building Vulnerability Assessment Checklist. The Risk Assessment Database is an integral part of this How-To Guide.

Using the Building Vulnerability Assessment Checklist and the Risk Assessment Database. For all types of evaluations (Tiers 1, 2, and 3) the Building Vulnerability Assessment Checklist and the Risk Assessment Database can be used to collect and report information related to the building infrastructure. In practice, many assessment Team members will find it easier to use a paper copy of the checklist while walking the site and enter their field observations when back in the office. The newer tablet personal computers (PCs) can be used for direct data entry. Typically, each assessment Team member will be responsible for completing several sections of the checklist; the amount and detail of information that can be acquired and inputted into the checklist will depend upon the on-site time available and the amount of information that is readily available versus difficult to find. For example, ideally, a full set of computer-aided design (CAD) drawings would be used to evaluate the site, architectural elements, structural features, mechanical and electrical systems, and security systems. However, if CAD drawings are not available, often the Disaster Management Office, Safety Officer, or building engineer will have 8½ x 11 inch site and floor plans that can be used in hard copy, scanned, and then color coded using simple photoshop applications. If no plans are available, a picture of the fire evacuation plan on each floor should be taken.

At the end of the day, after each assessment Team member has inputted his or her observations into the database, the Team should meet to review the observations and develop the vulnerability and mitigations list. The vulnerabilities can be grouped by campus, site, or individual building and each vulnerability can be given a priority; a vulnerability can have multiple mitigation options and each option should have a Rough Order of Magnitude Cost.

By reviewing the Critical Functions and Critical Infrastructure matrices and the color coded site and floor plans, the assessment Team can identify those functions and infrastructure that are collocated or are a single-point vulnerability (see Task 3.4) where multiple assets are susceptible to an event. A key risk reduction strategy is to build redundancy into the system by providing alternate means of service and places to connect temporary supplies for utilities and telecommunications, disperse or have alternate sites for key staff and functions, and have multiple means of communication for shelter-in-place and evacuation decisions.

Determining the Vulnerability Rating (Task 3.4)

This task involves determining a vulnerability rating that reflects the weakness of functions, systems, and sites in regard to a particular threat. Weakness includes the lack of redundancies that will make the building system operational after an attack.

Redundancy Factor

A terrorist selects the weapon and tactic that will cause harm to people, destroy the infrastructure, or functionally defeat the target. The function and infrastructure vulnerability analysis will identify the geographic distribution within the building and interdependencies between critical assets. Ideally, the functions should have geographic dispersion as well as a recovery site or alternate work location. However, some critical functions and infrastructure do not have a backup, or will be determined to be collocated and create what are called single-point vulnerabilities. Identification and protection of these single-point vulnerabilities is a key aspect of the assessment process. Concerns related to common system vulnerabilities are:

- No redundancy
- Redundant systems feed into single critical node
- Critical components of redundant systems collocated
- Inadequate capacity or endurance in post-attack environment

Identification and protection of these single-point vulnerabilities will help you to determine a more accurate vulnerability rating for your assessment. Figure 3-2 shows common system vulnerabilities.

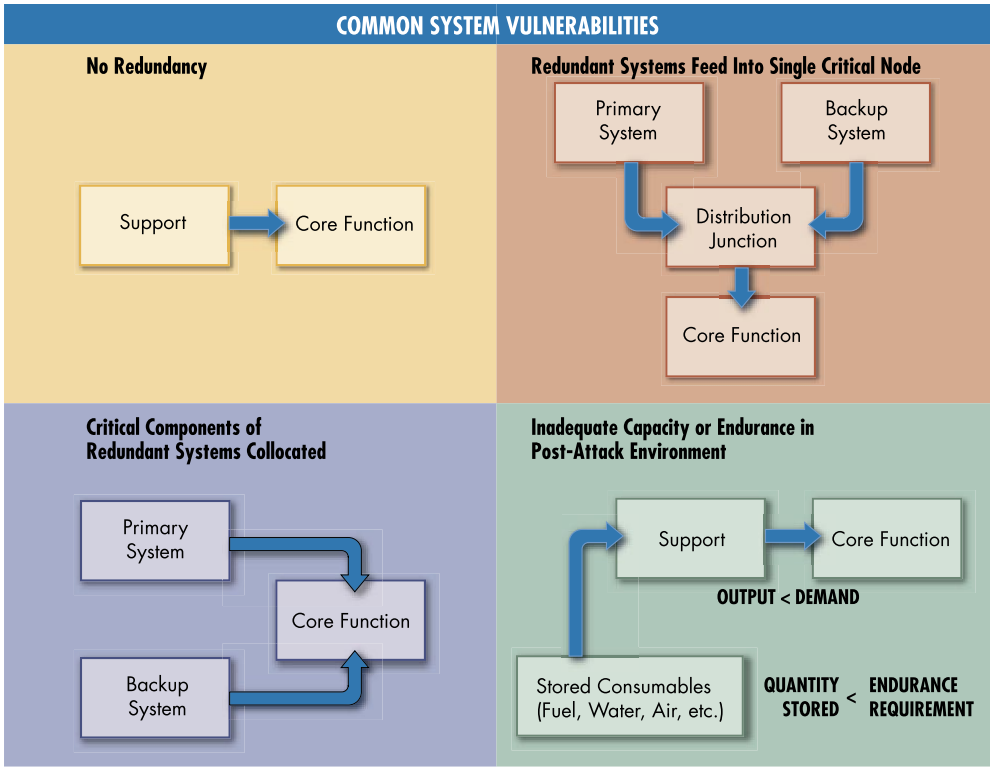


Figure 3-2 Common system vulnerabilities

Scale for Vulnerability Rating

For this How-To Guide, the following scale for vulnerability has been selected. Table 3-4 provides a scale for selecting your vulnerability rating. The scale is a combination of a 7-level linguistic scale and a 10-point numerical scale (10 being the greater threat). The key elements of this scale are the weaknesses of your building and easiness and/or difficulties that the aggressors may face when wishing to generate damage to your building. Also, the loss of operations in case of an attack and the lack of redundancies are considered. Tables 3-5A and 3-5B display a nominal example applying these ratings for an urban multi-story building.

Table 3-4: Vulnerability Rating

Criteria		
Very High	10	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 the entire building would be only functional again after a very long period of time after the attack.
High	8-9	High – One or more major 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 would be only functional again after a long period of time after the attack.
Medium High	7	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 most critical functions would be only operational again after a long period of time after the attack.
Medium	5-6	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 most part of the building would be only functional again after a considerable period of time after the attack.
Medium Low	4	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 most critical functions would be only operational again after a considerable period of time after the attack.
Low	2-3	Low – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated a good level of redundancies/physical protection and the building would be operational within a short period of time after an attack.
Very Low	1	Very Low – No weaknesses exist. The building has incorporated excellent redundancies/physical protection and the building would be operational immediately after an attack.

Table 3-5A: Nominal Example of Vulnerability Rating for a Specific Multi-story Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	7	7	9	9	9
Engineering	4	4	5	6	6
Warehousing	4	8	9	9	9
Data Center	5	4	3	4	4
Food Service	1	4	5	9	9
Security	5	5	10	9	9
Housekeeping	1	3	3	3	3
Day Care	3	9	9	9	9

Table 3-5B: Nominal Example of Vulnerability Rating for a Specific Multi-story Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	1	7	6	4	4
Architectural	1	9	7	2	2
Structural Systems	1	10	7	2	1
Envelope Systems	1	9	7	2	1
Utility Systems	2	6	2	2	1
Mechanical Systems	1	8	5	9	9
Plumbing and Gas Systems	1	6	3	6	2
Electrical Systems	7	8	6	2	1
Fire Alarm Systems	1	6	8	2	1
IT/Communications Systems	8	6	8	2	1

WORKSHEET 3-1: NOMINAL ASSESSMENT SCHEDULE

Assessment Schedule			
Location	**Team Members**	**Dates**	**Comments**
Building 1 Location:		First On-Site Visit	
		Second On-Site Visit	
		Third On-Site Visit	
Building 2 Location:		First On-Site Visit	
		Second On-Site Visit	
		Third On-Site Visit	
		Fourth On-Site Visit	

Contact Information			
Member	**Phone**	**E-mail**	**Comments**
Main Stakeholder			
Field Staff			
Team Member 1			
Team Member 2			
Team Member 3			

Worksheet 3-1 provides an example of a nominal assessment schedule for two buildings owned by the same stakeholder. It reflects a multi-day assessment with a variable number of Team members. The bottom of the table includes space to write key contact information. Remember that a Team can be contacted to perform assessments for multiple buildings.

WORKSHEET 3-2: ASSESSMENT AGENDA

Infrastructure	Site and Components to be Assessed	Members
Site		
Architectural		
Structural Systems		
Envelope Systems		
Utility Systems		
Mechanical Systems		
Plumbing and Gas Systems		
Electrical Systems		
Fire Alarm Systems		
IT/Communications Systems		

Worksheet 3-2 will help you to prepare your assessment agenda. Using the Building Vulnerability Assessment Checklist, the Team should propose the areas that need to be analyzed during the on-site visits. The proposed list will be discussed with building owners and facility managers and will be finalized by the Assessment Team.

WORKSHEET 3-3: VULNERABILITY RATING

Function	Vulnerability	Infrastructure	Vulnerability
Administration		Site	
Engineering		Architectural	
Warehousing		Structural Systems	
Data Center		Envelope Systems	
Food Service		Utility Systems	
Security		Mechanical Systems	
Housekeeping		Plumbing and Gas Systems	
Day Care		Electrical Systems	
Other		Fire Alarm Systems	
Other		IT/Communications Systems	

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

Worksheet 3-1 can be used to complete your risk assessment and will be used in conjunction with Worksheets 4-1 and 4-2. It can be used to discuss the vulnerability rating with building stakeholders and among the members of the Assessment Team. Vulnerability rating refers to a numerical value that can be assigned to building weaknesses and lack of redundancy.

To fill out Worksheet 3-1, analyze the impact of a particular threat to your site and/or building. Analyze core functions and building infrastructure components as indicated in Task 2.2 of Step 2. Analyze your assets based on: a) the identified threat; b) the criticality of your assets: and c) a level of protection you may have chosen (i.e., your willingness or unwillingness to accept risk). When assigning a vulnerability rating, consider redundancy factors included in Task 3.4. This may increase your vulnerability rating for functions and infrastructure.

STEP 4: RISK ASSESSMENT

OVERVIEW

The fourth step in the assessment process is to prepare a risk assessment for your site and building (see Figure 4-1). The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood of the threat occurring and the consequences of the occurrence.

The risk assessment process involves the following tasks:

- Preparing the risk assessment matrices
- Determining the risk ratings
- Prioritizing observations in the Building Vulnerability Assessment Checklist

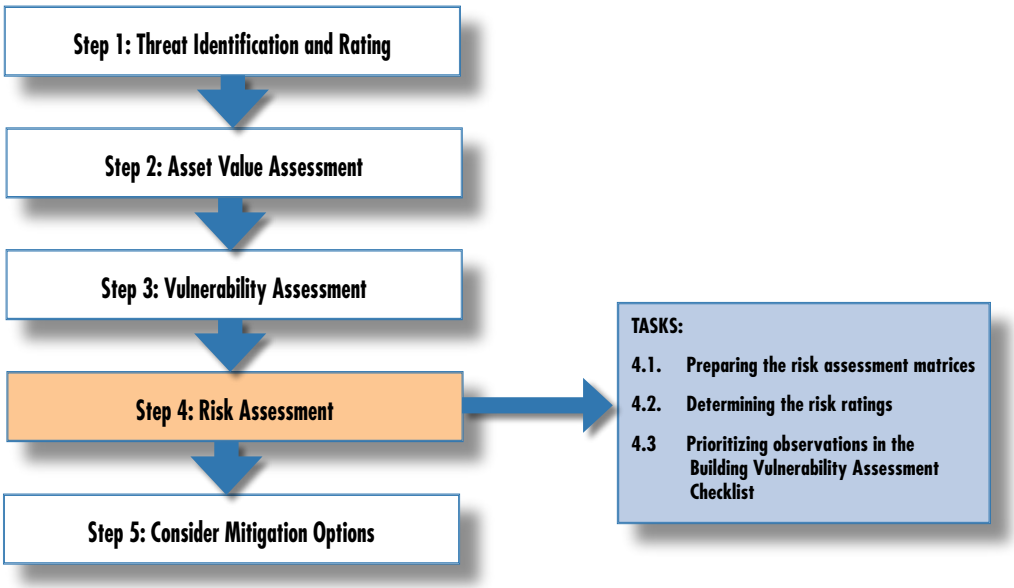


Figure 4-1 Steps and tasks

There are a number of methods and means to conduct a building risk assessment, and the steps can be accomplished in different sequences. However, they all have one common objective, which is to apply a quantitative assessment process that identifies those assets at highest risk and evaluate mitigation measures that can reduce that risk. The process selected for this How-To Guide is described below.

Preparing the Risk Assessment Matrices (Task 4.1)

In order to estimate potential losses, a series of matrices have been prepared. The inputs for these matrices are based on the analysis performed during Steps 1, 2, and 3.

To estimate risk, a number of factors need to be taken into consideration. The first one is to identify and rate the threats that could cause harm to a building and its inhabitants. Next, the value of assets and people that need to be protected will be identified. After threats and assets are identified, a vulnerability rating that identifies weaknesses that might be exploited by a terrorist or aggressor is determined. Risk can be computed using the results of the threat rating, asset value, and vulnerability rating.

Tables 4-1 to 4-10 can be used as a pre-assessment screening tool by the Team while conducting the on-site meetings with key staff members (e.g., building owners, security, site management, key function representatives, etc.). The tables should be completed by consensus judgment of the building stakeholders and Assessment Team members. The risk assessment matrices can provide both a quantitative score and color code to objectively and visually determine the functions and systems that have been determined to be at risk.

During Steps 1 and 2, you should have identified your threat rating (Worksheet 1-2), asset value (Worksheet 2-1), and vulnerability rating (Worksheet 3-3). At this point, you should transfer these values to Worksheets 4-1 and 4-2.

In the risk assessment matrices, the threats are listed across the top, and the functions and infrastructure are listed down the side to create threat-pairs. In general, there are two approaches to complete Worksheets 4-1 and 4-2. One approach is to start with all cell elements set to zero and discuss each element in detail to arrive at a consensus number. Another approach is to start with all cell elements equal to a numeric value (e.g., "5") and then adjust cell values up or down. With either approach, the first few rows and columns will take the longest time to reach consensus values, but, as the group becomes familiar with the ratings and scales, the process converges quickly. It should take approximately 3 to 4 hours to complete the matrices and, during that time, many of the building vulnerabilities will be verbally identified and collaborated with the vulnerability portfolio and earlier building site tour.

Identifying and Determining the Threat Rating. Step 1 will help you to identify and come to a consensus in terms of the threat rating. After each threat/hazard has been identified and defined, the threat level for each

threat/hazard shall be determined. The threat rating is a subjective judgment of a terrorist threat based on existence, capability, history, intentions, and targeting. The threat rating is a snapshot in time, and can be influenced by many factors, but the given threat value will typically be the same for each function (going down the columns). Organizations that are dispersed in a campus environment may have variations in ratings. For threat rating, a scale from 1-10 was assigned: 10 is considered very high; 8-9 is high; 7 is medium high; 5-6 is medium; 4 is medium low; 2-3 is low; and 1 is very low.

Rating the Asset Value. Step 2 will help you to determine the asset value rating for your site and/or building. After a building's assets requiring protection have been identified, they should be 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. There are a number of methods and means to conduct a building risk assessment, and the steps can be accomplished in different sequences, but the objective is to apply a quantitative assessment process that identifies those assets at highest risk and evaluate mitigation measures that can reduce that risk. For an asset value rating, a scale from 1-10 was assigned: 10 is considered very high; 8-9 is high; 7 is medium high; 5-6 is medium; 4 is medium low; 2-3 is low; and 1 is very low.

Assessing the Vulnerability. Step 3 will help you to determine the vulnerability rating for your site and/or building. After your threat rating and asset value rating have been identified, the vulnerability rating should be determined. Vulnerability rating requires identifying and rating the vulnerability of each asset-threat pair. An indepth vulnerability assessment of a building evaluates specific design and architectural features, and identifies all vulnerabilities of the building functions and building systems. In the vulnerability rating scale of 1 to 10, 1 means very low or no weaknesses exist, and 10 means one or more major weaknesses exist to make an asset extremely susceptible to an aggressor.

Critical Functions Asset Value. Table 4-1 depicts a portion of the site critical functions matrix. It lists the functions down the left side and threats across the top. The asset value rating is entered into the site critical functions matrix and begins the process of quantifying the risk elements. 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 subjective, and provides a guide to vulnerabilities and risks. The asset value under the engineering and administration functions is highlighted. For administration, a medium asset value (5) was assigned for

all threats. For engineering, a high asset rating (8) was determined for all threats.

Table 4-1: Critical Functions Asset Value

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value	5	5	5	5	5
Threat Rating					
Vulnerability Rating					
Engineering					
Asset Value	8	8	8	8	8
Threat Rating					
Vulnerability Rating					

Critical Infrastructure Asset Value. Table 4-2 depicts a portion of the site critical infrastructure matrix. It lists infrastructure down the left side and threats across the top. In general, the asset value for a given infrastructure asset is the same for all threats and is usually the economic cost of replacement. The value can be changed to reflect intangibles such as duration of loss, loss of production capability, etc. The asset value rating under the site and structural systems is highlighted. A medium low asset value rating (4) was assigned for the site infrastructure threat pairs. A high asset value rating (8) was assigned for the structural system threat pairs.

Table 4-2: Critical Infrastructure Asset Value

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value	4	4	4	4	4
Threat Rating					
Vulnerability Rating					
Structural Systems					
Asset Value	8	8	8	8	8
Threat Rating					
Vulnerability Rating					

Critical Functions Threat Rating. The threat rating under the site and structural systems is highlighted in Table 4-3. A high threat rating (8) was assigned for a cyber attack based on known groups releasing worms and viruses; a medium low threat rating (4) was assigned for a vehicle bomb; a medium threat rating (5) was assigned for a suicide bomber based on current intelligence on known groups and quantity of explosives available; and a low threat rating (2)

was assigned for both Sarin and Ricin attacks based on current intelligence of prior targets and predicted use against future targets (assuming that the building is not the primary target, but may experience collateral damage effects).

Table 4-3: Critical Functions Threat Rating

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating					
Engineering					
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating					

Critical Infrastructure Threat Rating. The threat rating under the site and structural systems is highlighted in Table 4-4. A high threat rating (8) was assigned for a cyber attack based on known groups releasing worms and viruses; a medium low threat rating (4) was assigned for a vehicle bomb; a medium threat rating (5) was assigned for a suicide bomber based on current intelligence on known groups and quantity of explosives available; and a low threat rating (2) was assigned for both Sarin and Ricin attacks based on current intelligence of prior targets and predicted use against future targets (assuming that the building is not the primary target, but may experience collateral damage effects).

Table 4-4: Critical Infrastructure Threat Rating

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating					
Structural Systems					
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating					

Critical Functions Vulnerability Rating. In Table 4-5, for administration, a medium high vulnerability rating (7) was determined for a cyber attack; a medium high vulnerability rating (7) was determined for a vehicle bomb; a

high vulnerability rating (9) was assigned for a suicide bomber, and for Sarin and Ricin attacks because administration is located at the lobby entrance. For engineering, a medium vulnerability rating (7) was determined for a cyber attack; a medium low vulnerability rating (4) was determined for a vehicle bomb; a medium vulnerability rating (5) was determined for a suicide bomber; and a medium vulnerability rating (6) was determined for a Sarin or Ricin attack.

Table 4-5: Critical Functions Vulnerability Rating

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value	5	5	5	5	5
Threat Rating	8	4	3	2	2
Vulnerability Rating	7	7	9	9	9
Engineering					
Asset Value	8	8	8	8	8
Threat Rating	8	5	6	2	2
Vulnerability Rating	7	4	5	6	6

Critical Infrastructure Vulnerability Rating. In Table 4-6, a low vulnerability rating (1) was determined for a cyber attack because there are no internet devices; a medium high vulnerability rating (7) was determined for a vehicle bomb; a low vulnerability rating (3) was determined for a suicide bomber; a low vulnerability rating (2) for Sarin and Ricin attacks because there would be little damage impact on the site. For structural systems, a low vulnerability rating (1) was determined for a cyber attack; a high vulnerability rating (10) was determined for a vehicle bomb due to progressive collapse concerns; a medium vulnerability rating (6) was determined for a suicide bomber who could place a device next to a primary support and load bearing column; and a low vulnerability rating (1) was determined for a Sarin or Ricin attack because there would be little or no damage.

Table 4-6: Critical Infrastructure Vulnerability Rating

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	7	3	2	2
Structural Systems					
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	10	6	1	1

Determining the Risk Ratings (Task 4.2)

Risk is the potential for a loss or damage to an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is based on the likelihood or probability of the hazard occurring and the consequences of the occurrence. A risk assessment analyzes the threat (probability of occurrence), asset value (consequences of the occurrence), and vulnerabilities to ascertain the level of risk for each asset against each applicable threat/hazard. The risk assessment provides engineers and architects with a relative risk profile that defines which assets are at the greatest risk against specific threats.

There are numerous methodologies and technologies for conducting a risk assessment. For this How-To Guide, the approach is to assemble the results of the threat assessment, asset value assessment, and vulnerability assessment, and determine a numeric value of risk for each asset and threat/hazard pair in accordance with the following formula:

Risk = Asset Value x Threat Rating x Vulnerability Rating

To prepare the risk estimation matrices three factors or elements of risk are considered for each function or system against each threat previously identified. Multiplying the values assigned to each of the three factors provides quantification of total risk. The total risk for each function or system against each threat is assigned a color code. The results of the risk assessment should be used to help prioritize which mitigation measures should be adopted, given limited resources, in order to achieve a desired level of protection. To determine your risk rating, you may use Table 4-7, which includes information on observations in the Building Vulnerability Assessment Checklist (Appendix A) on the total risk scale and color codes. A site functional pre-screening matrix is shown in Table 4-8 and a site infrastructure pre-screening matrix is

shown in Table 4-9. Worksheets 4-1 and 4-2 will assist you in preparing and organizing the information for your risk assessment.

Table 4-7: Total Risk Scale Color Code

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

Table 4-8: Site Functional Pre-Assessment Screening Matrix

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	280	140	225	90	90
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	7	9	9	9
Engineering	448	128	200	96	96
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	6	6
Warehousing	168	96	135	54	54
Asset Value	3	3	3	3	3
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	9	9	9
Data Center	320	128	120	64	64
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	5	4	3	4	4
Food Service	112	32	50	36	36
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	9	9
Security	392	140	350	126	126
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	5	10	9	9
Housekeeping	112	24	30	12	12
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	3	3	3	3
Day Care	504	324	405	162	162
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	9	9	9	9

Table 4-9: Site Infrastructure Pre-Assessment Screening Matrix

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	32	128	60	16	16
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	7	3	4	4
Architectural	40	180	175	20	20
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	9	7	2	2
Structural Systems	64	320	240	32	32
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	10	6	2	1
Envelope Systems	56	252	210	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	9	6	2	1
Utility Systems	112	168	70	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	2	6	2	2	1
Mechanical Systems	56	224	175	126	126
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	8	5	9	9
Plumbing and Gas Systems	40	120	75	60	20
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	6	3	6	2
Electrical Systems	392	224	210	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	6	2	1
Fire Alarm Systems	72	216	320	36	18
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	6	8	2	1
IT/Communications Systems	512	192	240	32	16
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	8	6	6	2	1

Prioritizing Observations in the Building Vulnerability Assessment Checklist (Task 4.3)

The Building Vulnerability Assessment Checklist relates to building core infrastructure. During Task 3.3, the Assessment Team performed an on-site assessment and filled out observations in the Building Vulnerability Assessment Checklist. (Table 4-10 provides a nominal example.) As mentioned before, the Checklist is a key tool in the preparation of the vulnerability assessment. It is used to guide the assessors performing the assessment of the facility. The vulnerabilities of the facility are selected from the observations provided for each vulnerability question. These vulnerabilities are then prioritized to determine the most effective mitigation measures. Prioritization is based on the greatest vulnerabilities that can be exploited by the aggressors and largest risks in terms of loss of lives, building damage, and loss of operation. Task 4.3 is the final task of the risk assessment. It allows the assessors to rank their observed facility vulnerabilities and proposed remedial actions. Worksheet 4-3 will help you to perform this task. For more information on how to use the Building Vulnerability Assessment Checklist, see Step 3 and Appendix A.

Table 4-10: Nominal Example of Observations in the Building Vulnerability Assessment Checklist

Section	Vulnerability Question	Guidance	Observations
1.	**Site**		
	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*	The main gate entrance remains wide open for vehicle and pedestrian intruders. There are missing street signs throughout the facility. It is difficult to channel staff and visitors to control access points. There is only one security vehicles to serve the entire campus; at least two more are required.
2.	**Architectural**		
2.27	**Is interior glazing near high-risk areas minimized?** **Is interior glazing in other areas shatter-resistant?**	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. Reference: *GSA PBS-P100*	In the main facade, windows are not blast-resistant and the glass is not properly anchored to the frame. In case of a blast event, it is anticipated that the glass will break and will not remain in the frame. This could cause extensive injuries in case of an explosive event.
8.	**Utility Systems**		
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*	There are single-point vulnerabilities to the steam and electricity lines. Any damage to the steam or electric lines would result in loss of utilities.

WORKSHEET 4-1: SITE FUNCTIONAL PRE-ASSESSMENT MATRIX

Worksheet 4-1 can be used to complete your risk assessment by determining the functions at a higher risk. To fill out this matrix, use the scales and color codes, provided in Steps 4.1 and 4.2 .

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

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration					
Asset Value					
Threat Rating					
Vulnerability Rating					
Engineering					
Asset Value					
Threat Rating					
Vulnerability Rating					
Warehousing					
Asset Value					
Threat Rating					
Vulnerability Rating					
Data Center					
Asset Value					
Threat Rating					
Vulnerability Rating					
Food Service					
Asset Value					
Threat Rating					
Vulnerability Rating					
Security					
Asset Value					
Threat Rating					
Vulnerability Rating					
Housekeeping					
Asset Value					
Threat Rating					
Vulnerability Rating					
Day Care					
Asset Value					
Threat Rating					
Vulnerability Rating					

WORKSHEET 4-2: SITE INFRASTRUCTURE SYSTEMS PRE-ASSESSMENT MATRIX

Worksheet 4-2 can be used to complete your risk assessment by determining the infrastructure at a higher risk.

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site					
Asset Value					
Threat Rating					
Vulnerability Rating					
Architectural					
Asset Value					
Threat Rating					
Vulnerability Rating					
Structural Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Envelope Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Utility Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Mechanical Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Plumbing and Gas Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Electrical Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
Fire Alarm Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					
IT/Communications Systems					
Asset Value					
Threat Rating					
Vulnerability Rating					

WORKSHEET 4-3: PRIORITIZATION OF OBSERVATIONS IN THE CHECKLIST

The observations you made in the Building Vulnerability Checklist (Appendix A) during Step 3 should now be used to review the vulnerability ratings in Worksheets 4-1 and 4-2, and then the risk ratings for the associated Threat-Asset Pairs in those worksheets. The observations that you use to confirm or adjust the vulnerability ratings are your selected vulnerabilities that Worksheet 4-3 can help you prioritize. The top portion of Worksheet 4-3 should have the selected observations/vulnerabilities listed in the Cross Reference Column. Using the updated results of Worksheets 4-1 and 4-2, indicate all high risk (red) Functions and Infrastructure column-row intersections that the vulnerability in the Cross Reference Column impacts. As previously stated, prioritization is based on the greatest vulnerabilities that can be exploited by the aggressors and largest risks in terms of loss of lives, building damage, and loss of operation. The bottom portion of Worksheet 4-3 should contain your selected observations/vulnerabilities that meet this statement in rank order – highest to lowest. For example, Ranked Observation 1 would have the highest vulnerability rating matched with the highest risk rating and impacting the greatest number of Functions and Infrastructure. This table can be expanded to include more observations, as needed. In the Risk Assessment Database, vulnerabilities can be given a priority of 1 to 5 as defined by the Manager prior to the assessment. For example, the priority could be based upon the speed in which the vulnerability should be mitigated, or needed level of risk reduction sought, or ability to be exploited by the aggressor, etc.

Cross Reference	Functions	Administration	Engineering	Warehousing	Data Center	Food Service	Security	Housekeeping	Day Care	Infrastructure	Site	Architectural	Structural Systems	Envelope Systems	Utility Systems	Mechanical Systems	Plumbing and Gas Systems	Electrical Systems	Fire Alarm Systems	IT/Communications Systems
Observation 1																				
Observation 2																				
Observation 3																				
Observation 4																				
Observation 5																				
Observation 6																				
Ranked Observations																				
Observation 1																				
Observation 2																				
Observation 3																				
Observation 4																				
Observation 5																				
Observation 6																				

STEP 5: CONSIDER MITIGATION OPTIONS

OVERVIEW

The fifth step in this How-To Guide is to identify and evaluate various mitigation options that are directly associated with, and responsive to, the major risks identified during Step 4 (see Figure 5-1). After the risk assessment process is completed, the stakeholders are frequently left with several areas where assets require mitigation measures and are limited by factors discussed in this step. Thus, decisions need to be made to focus the available resources on the most practical mitigation options.

The consider mitigation options process involves the followings tasks:

- Identifying preliminary mitigation options
- Reviewing mitigation options
- Estimating cost
- Reviewing mitigation options, cost, and the layers of defense

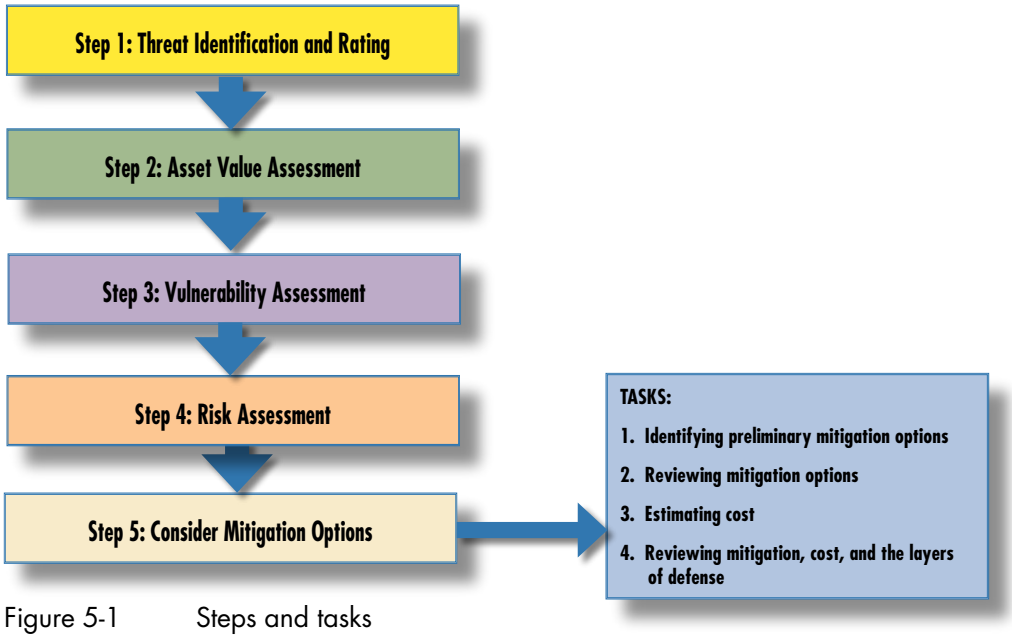


Figure 5-1 Steps and tasks

Step 5 emphasizes mitigation measures that can reduce the destructive effects against buildings in case of a terrorist attack. During this step, you will examine the mitigation options from the point of view of their effectiveness, acceptability, and feasibility with respect to prevailing implementation condi-

tions. The proposed procedure for examining the mitigation options is not meant to replace full and thorough analysis of the technical assessment; it is meant to help you narrow down your options and focus your attention on those measures that have the greatest chance of effective implementation.

Worksheets 4-3, 5-1, and 5-2 and the Building Vulnerability Assessment Checklist (Appendix A) should be used for the preparation of your mitigation options.

In order to identify, select, and implement the most appropriate mitigation measures, general mitigation goals and objectives, and the merits of each potential mitigation measure should be examined. The building owner may take the final decision regarding which mitigation measures should be implemented. However, engineers, architects, landscape architects, and other technical people should be involved in this process to ensure that the results of the risk assessment are met with sound mitigation measures that will increase the capability of the building to resist potential terrorist attacks.

To select, evaluate, and prioritize potential mitigation options, this How-To Guide has selected criteria that help to answer the following questions:

- Which mitigation measures are most appropriate for the types of risks faced by your assets?
- Are resources and capabilities sufficient to implement these measures and what additional resources might be needed?
- What impacts will the implementation of these measures have in areas surrounding your building(s) or in your community?

Identifying Preliminary Mitigation Options (Task 5.1)

After the Assessment Team and building stakeholders know which assets are at greatest risk (see Step 4), they can then identify mitigation measures to reduce this risk. Because it is not possible to completely eliminate risk and every project has resource limitations, you must carefully analyze your mitigation options. Worksheet 5-1 and the remaining sections of Task 5.1 will help you to identify your preliminary mitigation options.

Prioritized Observations from the Building Vulnerability Assessment Checklist

The Building Vulnerability Assessment Checklist (Appendix A) is the main source for identifying mitigation options. To identify your mitigation options you should start with the observations made in the Checklist when conducting the on-site assessment (see Task 3.2), but use your expertise and experience during the assessment to determine any vulnerabilities or mitigation options that may not be covered in the standard process. Then prioritize these observations as vulnerabilities (see Task 4.3). The remaining part of this task will help you to create a feasible framework for the identified observations.

Regulatory Measures, Rehabilitation of Existing Structures, and Protective and Control Structures Parameters

Mitigation measures can be viewed from many different perspectives. In this How-To Guide, the emphasis is on addressing building infrastructure and core building functions. The purpose is to identify sound mitigation measures directed at reducing the effects of potential terrorist attacks on the built environment. For this task, three broad categories have been identified:

- Regulatory measures
- Repair and strengthening of existing structures
- Protective and control measures

Regulatory Measures. Regulatory measures include legal and other regulatory instruments that governments use to prevent, reduce, or prepare for the losses associated with manmade hazard events that affect commercial buildings, which are the central topic of this How-To Guide. Examples include:

- Legislation that organizes and distributes responsibilities to protect a community from manmade threats
- Regulations that reduce the financial and social impact of manmade hazards through measures, such as insurance
- New or updated design and construction codes
- New or modified land use and zoning regulations

- Incentives that provide inducements for implementing mitigation measures

In most cases, regulatory measures should be considered before implementing other measures because regulatory measures provide the framework for decision-making, organizing, and financing of mitigation actions.

Repair and Strengthening of Existing Structures. As its name implies, repair and strengthening deals with structural and non-structural modifications of existing buildings and infrastructure facilities. Although new construction can include protective measures to reduce the potential impact against terrorist attacks, existing buildings may be at risk because they were constructed without the appropriate safety measures to withstand potential terrorist attacks. Thus, improving the safety and structural integrity of existing buildings and infrastructure facilities is often the best way to reduce the impact of manmade events on such structures.

When a manmade hazard occurs, it can directly damage a target building or indirectly cause secondary effects in adjacent buildings. The level of damage is impacted by each structure's quality of design and construction. Poorly engineered and constructed buildings are usually not able to resist the forces generated by a blast event or serve as safe havens in case of CBR attacks.

Protective and Control Measures. Unlike other mitigation measures that improve the resistance of buildings and infrastructure to disasters, protective and control measures focus on protecting structures by deflecting the destructive forces from vulnerable structures and people.

Ideally, a potential terrorist attack is prevented or pre-empted through intelligence measures. If the attack does occur, physical security measures combine with operational forces (e.g., surveillance, guards, and sensors) to provide layers of defense that delay and/or thwart the attack (for more information, see Task 2.1). Deception may be used to make the facility appear to be a more protected or lower-risk facility than it actually is, thereby making it a less attractive target. Deception can also be used to misdirect the attacker to a portion of the facility that is non-critical. As a last resort, structural hardening is provided to save lives and facilitate evacuation and rescue by preventing building collapse and limiting flying debris.

Because of the interrelationship between physical and operational security measures, it is imperative for the owner and security professional to define, early in the design process, what extent of operational security is planned for

various threat levels. If properly implemented, physical security measures will contribute toward the goals listed below in prioritized order.

- **Preventing an attack.** By making it more difficult to implement some of the more obvious attack scenarios (such as a parked car in the street) or making the target appear to be of low value in terms of the amount of sensation that would be generated if it were attacked, the would-be attacker may become discouraged from targeting the building. On the other hand, it may not be advantageous to make the facility too obviously protected or not protected, because this may provide an incentive to attack the building.

- **Delaying the attack.** If an attack is initiated, properly designed landscape or architectural features can delay its execution by making it more difficult for the attacker to reach the intended target. This will give the security forces and authorities time to mobilize and possibly stop the attack before it is executed. This is done by creating a buffer zone between the publicly accessible areas and the vital areas of the facility by means of an obstacle course, a serpentine path, or a division of functions within the facility. Alternatively, through effective design, the attacker could be enticed to a non-critical part of the facility, thereby delaying the attack.

- **Mitigating the effects of the attack.** If these precautions are implemented and the attack still takes place, structural protection efforts will serve to control the extent and consequences of damage. In the context of the overall security provided to the building, structural protection is a last resort that only becomes effective after all other efforts to stop the attack have failed. In the event of an attack, the benefits of enhancements to life-safety systems may be realized in lives saved.

The goal of the assessment process is to achieve the level of protection sought through implementation of mitigation measures in the building design. These measures may reduce risk by deterring, detecting, denying, or devaluing the potential threat element prior to or during execution of an enemy attack. The Department of Homeland Security uses the following methodology to achieve this purpose.

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

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

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

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

Reviewing Mitigation Options (Task 5.2)

At this point, you should have identified a preliminary list of mitigation options. These options should have been grouped under the regulatory, rehabilitation, and protective and control framework for blast and CBR. The remaining sections of Task 5.2 provide a set of criteria to help you to narrow down the mitigation options identified during Task 5.1. Worksheet 5-2 will help you to analyze further your mitigation options in order to select those that are more feasible to be implemented. The selected criteria include the following:

Available Political Support

Political support involves examining the proposed mitigation options by seeking the opinions of local and State elected officials, as well as the community as a whole. Most communities have learned that success of mitigation efforts hinges on political- and community-wide support. Building an effective political constituency for implementation of mitigation measures in most cases requires time and patience. However, some mitigation options will garner such support more easily than others.

Community Acceptance

Community acceptance cannot be viewed separately from the need for political support for the proposed mitigation options. Both are necessary preconditions for their successful implementation. In many cases, community-wide campaigns are necessary to explain the risks, the reasons for, and the expected benefits from the proposed measures.

Cost

Although the implementation of mitigation measures hinges on political commitment and technical capacity, it also depends heavily on the costs involved. After identifying your mitigation measures in Task 5.1, you will have some idea of the cost involved and opportunities for implementation.

Benefit

When implementing a mitigation measure, it is important to consider that the benefit of implementing the option outweighs the cost. After identifying your mitigation measures in Task 5.1, you will have some idea of the benefits that may result from implementing your mitigation measures.

Available Financial Resources

As you begin Task 5.2, it is important to have some knowledge of the available resources for implementing mitigation options. The Team should discuss this issue with the site and building owners because the amount of financial resources may define the type of mitigation options to be adopted. The Team should also discuss any Federal and State programs available for financing large-scale mitigation measures.

Legal Authority

Without the appropriate legal authority, a mitigation action cannot lawfully be undertaken. You will need to determine whether the building owner has the legal authority to implement the selected mitigation options or whether it is necessary to wait for new laws or regulations. For example, creating stand-off distances in urban areas can be against zoning ordinances and building set-back requirements.

Adversely Affected Population

While implementing your mitigation measures to solve problems related to blast and CBR resistance, you may want to consider that some segments of the population may be adversely affected. For example, the construction of barriers and bollards can inhibit the number of tourists visiting a particular city and might affect the community and the hospitality sector.

Adverse Effects on the Already Built Environment

Some mitigation measures may have a negative effect on the already built environment. When selecting mitigation measures, the following should be strictly scrutinized:

- Effects on traffic/vehicular mobility
- Effects on pedestrian mobility
- Effects on ingress and egress to the building
- Effects on other building operations
- Effects on aesthetics
- Potential interference with first responders

Impact on the Environment

When considering mitigation options, it is important to consider whether the recommended mitigation options will have a negative effect on environmental assets such as threatened and endangered species, wetlands, and other protected natural resources.

Technical Capacity

Some mitigation measures require highly skilled and specialized engineering expertise for implementation. Although experts can be hired on a short-term basis, the technical complexity of some mitigation solutions may require the expertise for long-term maintenance. It is therefore necessary to examine the technical capacities of all stakeholders and identify key technical expertise needed for each proposed mitigation option. If adequate technical capabilities are available for proposed mitigation measures, you should rank them higher on your priority list.

Funding for Maintenance and Operations

When considering the implementation of your mitigation options, you should be sure that funding is available for maintenance and operations.

Ease and Speed of Implementation

Different mitigation measures require different kinds of authority for their implementation. The Team must identify public authorities and responsible agencies for implementing mitigation measures and must examine their rules and regulations. The Team must identify all legislative problem areas and institutional obstacles as well as the incentives that can facilitate mitigation and implementation. The Team will have to balance the desirability of the mitigation measure against the community's rules and regulations in order to decide which takes precedence.

Timeframe and Urgency

Some mitigation measures require immediate implementation due to their nature (i.e., repetitive security breaches), political desire (i.e., platform project), or social perception (i.e., recent damage and disaster) of the risk. These perceptions can be the drivers to determining the timeframe for implementation of your mitigation options.

Short-term Solutions/Benefits

When considering your mitigation options, you may want to evaluate your

short-term solutions (i.e., mitigation options that will solve a particular problem temporarily, but may require additional funding in the future for follow-on projects). A short-term solution can be quickly accomplished and can demonstrate immediate progress in satisfying your community needs.

Long-term Solutions/Benefits

When considering your mitigation options, you may want to evaluate your long-term solutions (i.e., mitigation options that cannot be funded immediately, but will solve the problem permanently in the future when funds are available). A long-term solution can be more cost-effective in the long run that a short-term one.

Estimating Cost (Task 5.3)

The initial construction cost of protection has two components: fixed and variable. Fixed costs include such items as security hardware and space requirements. These costs do not depend on the level of an attack (i.e., it costs the same to keep a truck away from a building regardless of whether the truck contains 500 or 5,000 pounds of TNT). Blast protection, on the other hand, is a variable cost. It depends on the threat level, which is a function of the explosive charge weight and the stand-off distance. Building designers have no control over the amount of explosives used, but are able to change the level of protection by defining an appropriate stand-off distance, adopting hardening measures for their buildings, and providing sacrificial spaces that can be affected by terrorist attacks, but, at the same time, can protect people and critical building functions and infrastructure.

The optimal stand-off distance is determined by defining the total cost of protection as the sum of the cost of protection (construction cost) and the cost of stand-off (land cost). These two costs are considered as a function of the stand-off for a given explosive charge weight. The cost of protection is assumed to be proportional to the peak reflected pressure at the building envelope while the cost of land is proportional to the square of the stand-off distance. The optimal level of protection is the one that minimizes the sum of these costs.

If additional land is not available to move the secured perimeter farther from the building, the required floor area of the building can be distributed among additional floors. As the number of floors is increased, the footprint decreases, providing an increased stand-off distance. By balancing the increasing cost of the structure (due to the added floors) and the corresponding decrease in protection cost (due to added stand-off), it is possible to

find the optimal number of floors to minimize the cost of protection.

These methods for establishing the best stand-off distance are generally used for the maximum credible explosive charge. If the cost of protection for this charge weight is not within the budgetary constraints, the design charge weight must be modified. A study can be conducted to determine the largest explosive yield and corresponding level of protection that can be incorporated into the building, given the available budget.

Although it is difficult to assign costs to different upgrade measures because they vary, based on the site-specific design, some generalizations can be made (see Figure 5-2). Below is a list of enhancements arranged in order from least expensive to most expensive:

- Hardening of unsecured areas
- Measures to prevent progressive collapse
- Exterior window and wall enhancements

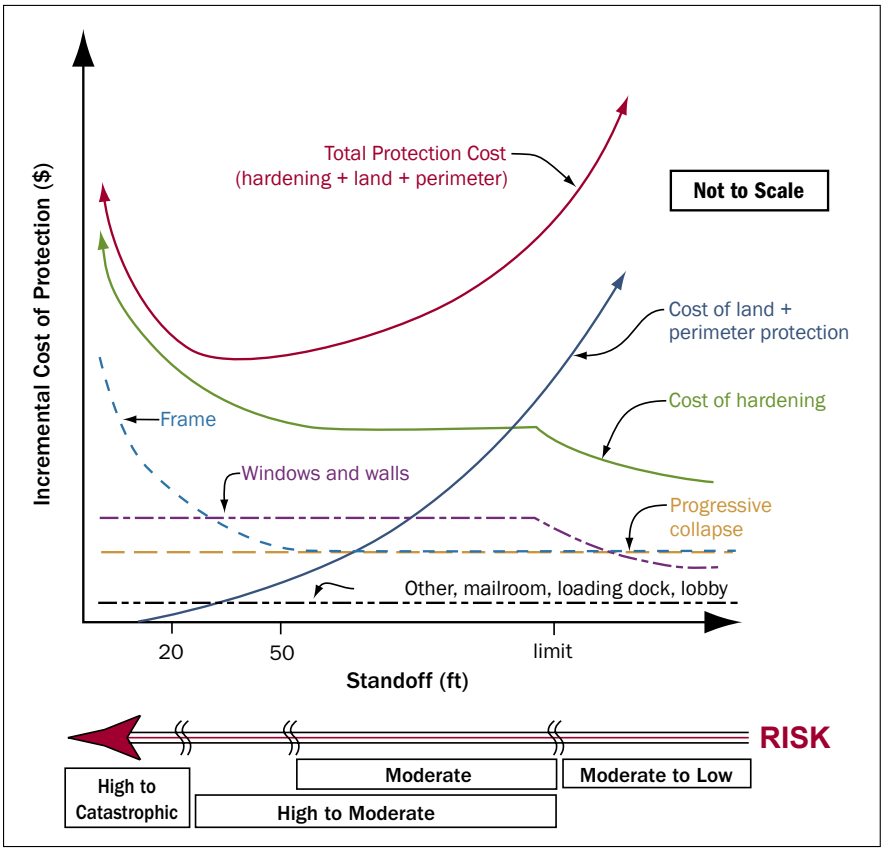


Figure 5-2 Cost considerations

Life-Cycle Costs

Life-cycle costs need to be considered as well. For example, if it is decided that two guarded entrances will be provided, one for visitors and one for employees, they may cost more during the life of the building than a single well designed entrance serving everyone. Also, maintenance costs may need to be considered. For instance, the initial costs for a CBR detection system may be modest, but the maintenance costs are high. Finally, if the rentable square footage is reduced as a result of incorporating robustness into the building, this may have a large impact on the life-cycle costs.

NIST PUBLICATIONS

For more information on life-cycle cost, see: NISTIR 7025, *Applications of Life-Cycle Cost Analysis to Homeland Security Issues in Constructed Facilities: A Case Study*, and NISTIR 7073, *Cost-Effective Responses to Terrorist Risks in Constructed Facilities*.

For more information on setting priorities, see: NIST GCR 04-865, *Best Practices for Project Security*, and NIST GCR 04-871, *Risk Analysis for Extreme Events: Economic Incentives for Reducing Future Losses*.

Electronic copies of these reports are available at *www.bfrl.nist.gov/oae/oae.html*.

Setting Priorities

If the costs associated with mitigating manmade hazards are too high there are three approaches available that can be used to combination: (1) reduce the design threat, (2) reduce the level of protection, or (3) accept the risk. In some cases, the owner may decide to prioritize enhancements, based on their effectiveness in saving lives and reducing injuries. For instance, measures against progressive collapse are perhaps the most effective actions that can be implemented to save lives and should be considered above any other upgrades. Laminated glass is perhaps the single most effective measure to reduce extensive non-fatal injuries. If the cost is still considered too great, and the risk is high because of the location or the high-profile nature of the building, then the best option may be to consider building an unobtrusive facility in a lower-risk area instead. In some cases (e.g., financial institutions with trading floors), business interruption costs are so high they outweigh all other concerns. In such a case, the most cost-effective solution may be to provide a redundant facility.

Early consideration of manmade hazards will significantly reduce the overall cost of protection and increase the inherent protection level provided to the building. If protection measures are considered as an afterthought or not considered until the design is nearly complete, the cost is likely to be greater, because more areas will need to be structurally hardened. An awareness of the threat of manmade hazards from the beginning of a project also helps the Team to determine early in the process what the priorities are for the facility. For instance, if extensive teak paneling of interior areas visible from the exterior is desired by the architect for the architectural expression of the building,

but the cost exceeds that of protective measures, then a decision needs to be made regarding the priorities of the project. Including protective measures as part of the discussion regarding trade-offs early in the design process often helps to clarify such issues.

Applicability of Benefit/Cost to Terrorist Threats

When prioritizing hazard mitigation alternatives, a benefit/cost analysis is generally conducted for each proposed action. A benefit/cost analysis involves calculating the costs of the mitigation measure and weighing them against the intended benefits, frequently expressed as losses avoided. However, applying benefit/cost analysis to terrorist threats can be challenging due to the following three main factors (for more information on this subject, see FEMA 386-7, *Integrating Human-Caused Hazards Into Mitigation Planning)*:

The probability of an attack or frequency is not known. The frequency factor is much more complex in the case of manmade hazards than for natural hazards. Although it is possible to estimate how often many natural disasters will occur (i.e., a structure located in the 100-year floodplain is considered to have a 1 percent chance of being flooded in any given year), it is very difficult to quantify the likelihood of a terrorist attack or technological disaster. Quantitative methods to estimate these probabilities are being developed, but have not yet been refined to the point where they can be used to determine incident probability on a facility-by-facility basis. The Assessment Team may use a qualitative approach based on threat and vulnerability considerations to estimate the relative likelihood of an attack or accident rather than the precise frequency. Such an approach is necessarily subjective, but can be combined with quantitative estimates of cost-effectiveness (the cost of an action compared to the value of the lives and property it saves in a worst-case scenario) to help illustrate the overall risk reduction achieved by a particular mitigation action.

The deterrence rate may not be known. The deterrence or preventive value of a measure cannot be calculated if the number of incidents it averts is not known. Deterrence in the case of terrorism may also have a secondary impact in that, after a potential target is hardened, a terrorist may turn to a less protected facility, changing the likelihood of an attack for both targets.

The lifespan of the action may be difficult to quantify. The lifespan of a mitigation action presents another problem when carrying out a benefit/cost analysis for terrorism and technological hazards. Future benefits are generally calculated for a natural hazard mitigation action in part by estimating the number of times the action will perform successfully over the course of its

useful life. However, some protective actions may be damaged or destroyed in a single manmade attack or accident. For example, blast-resistant window film may have performed to 100 percent effectiveness by preventing injuries from flying glass, but it may still need replacement after one "use." Other actions, such as a building setback, cannot be "destroyed" or "used up" per se. This is in contrast to many natural hazard mitigation actions, where the effectiveness and life span of a structural retrofit or land use policy are easily understood and their value over time is quantifiable.

Improving the Accuracy of your Cost Estimates

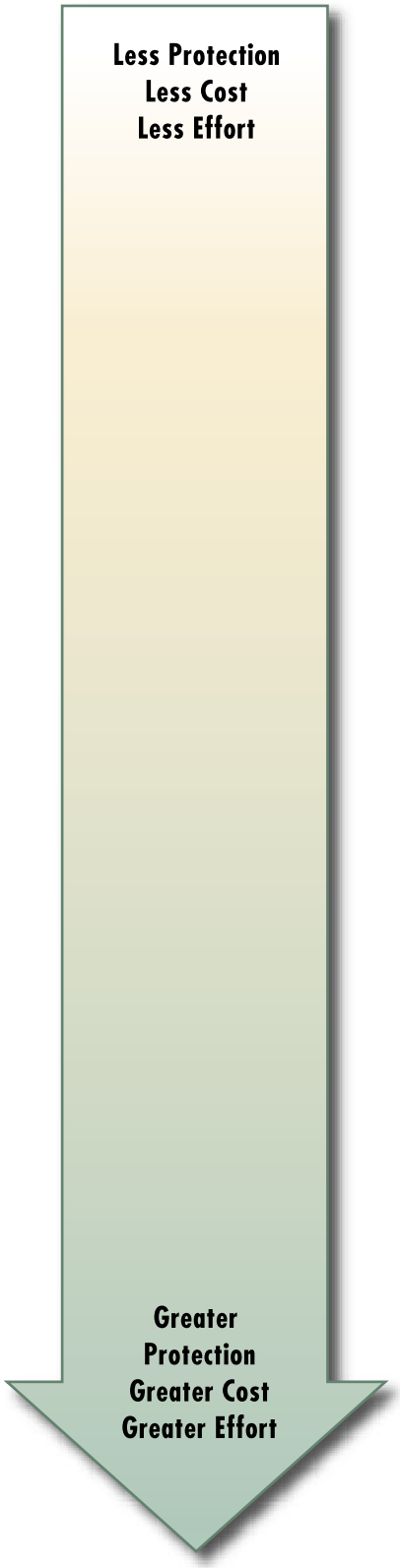
To improve the accuracy of your cost estimates, consult the Building Vulnerability Assessment Checklist in Appendix A. The Checklist follows the Construction Specifications Institute (CSI) format and cost estimates for infrastructure and equipment can be developed using industry standard applications and processes. Costing of mitigation options of physical security systems, blast-resistant materials and fixtures, and CBR protective sensors and devices is an emerging practice. A companion text to Appendix A is the RS Means Building Security; Strategies and Costs, which provides both a manual and an electronic costing approach.

Risk Assessment Database

The Risk Assessment Database provides a simple cost field for each mitigation option and cost summary reporting capability. Appendix B provides an extensive explanation on the subject.

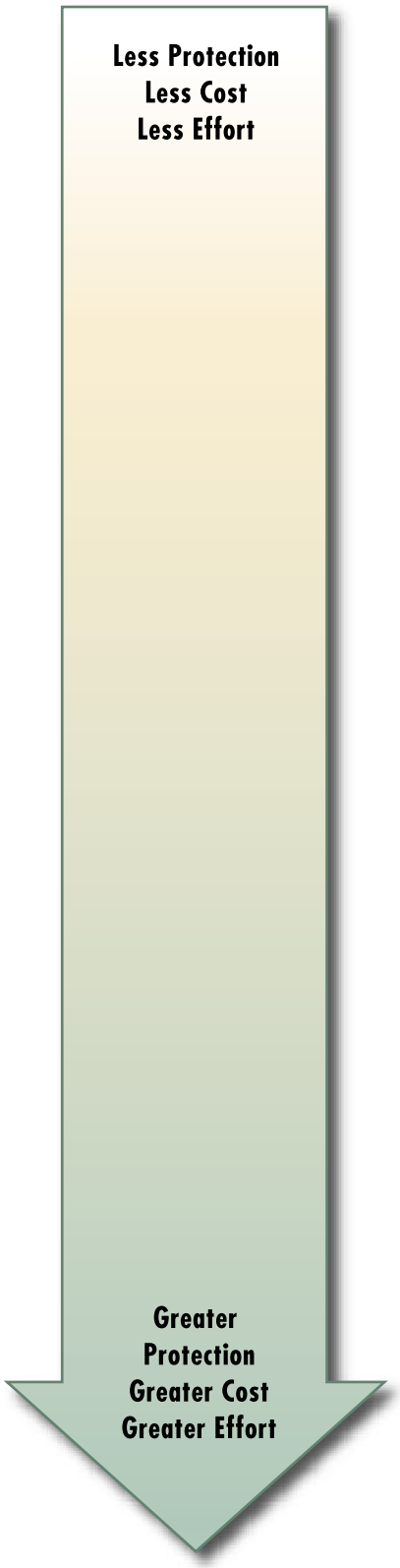
Mitigation, Cost, and the Layers of Defense (Task 5.4)

A general spectrum of site mitigation measures ranging from the least protection, cost, and effort to the greatest protection, cost, and effort are provided in Figures 5-3 and 5-4. These mitigation measures have been arranged by layers of defense (second and third layers), following the principle that the layers of defense create a succeeding number of security layers more difficult to penetrate. The underlying purpose of this task is to provide you with examples of mitigation measures for each layer and give you a broad idea on the potential correlation between protection and cost.



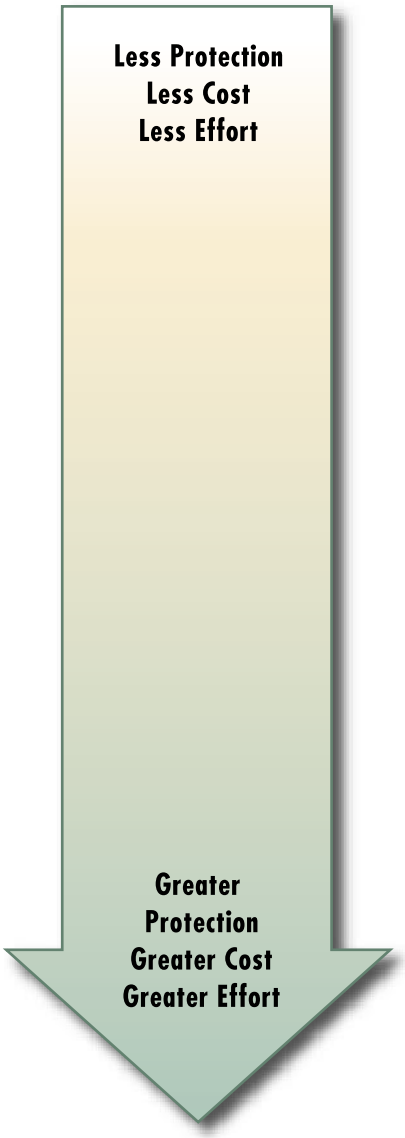
- Place trash receptacles as far away from the building as possible.
- Remove any dense vegetation that may screen covert activity.
- Use thorn-bearing plant materials to create natural barriers.
- Identify all critical resources in the area (fire and police stations, hospitals, etc.).
- Identify all potentially hazardous facilities in the area (nuclear plants, chemical labs, etc.).
- Use temporary passive barriers to eliminate straight-line vehicular access to high-risk buildings.
- Use vehicles as temporary physical barriers during elevated threat conditions.
- Make proper use of signs for traffic control, building entry control, etc. Minimize signs identifying high-risk areas.
- Introduce traffic calming techniques, including raised crosswalks, speed humps and speed tables, pavement treatments, bulbouts, and traffic circles.
- Identify, secure, and control access to all utility services to the building.
- Limit and control access to all crawl spaces, utility tunnels, and other means of under building access to prevent the planting of explosives.
- Utilize Geographic Information Systems (GIS) to assess adjacent land use.
- Provide open space inside the fence along the perimeter.
- Locate fuel storage tanks at least 100 feet from all buildings.
- Block sight lines through building orientation, landscaping, screening, and landforms.
- Use temporary and procedural measures to restrict parking and increase stand-off.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much stand-off distance as possible from potential vehicle bombs.
- Separate redundant utility systems.
- Conduct periodic water testing to detect waterborne contaminants.
- Enclose the perimeter of the site. Create a single controlled entrance for vehicles (entry control point).
- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed circuit television cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate stand-off for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Do not site the building adjacent to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas with minimum stand-off, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. In extreme cases, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or through street closings. For this measure, you need to work with your local officials.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.

Figure 5-3 Mitigation options for the second layer of defense



- Install active vehicle crash barriers. Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- Secure roof access hatches from the interior. Prevent public access to building roofs.
- Restrict access to building operation systems.
- Conduct periodic training of HVAC operations and maintenance staff.
- Evaluate HVAC control options.
- Install empty conduits for future security control equipment during initial construction or major renovation.
- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
- Minimize interior glazing near high-risk areas.
- Establish emergency plans, policies, and procedures.
- Establish written plans for evacuation and sheltering in place.
- Illuminate building access points.
- Restrict access to building information.
- Secure HVAC intakes and mechanical rooms.
- Limit the number of doors used for normal entry/egress.
- Lock all utility access openings.
- Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
- Install an internal public address system.
- Stagger interior doors and offset interior and exterior doors.
- Eliminate hiding places.
- Install a second and separate telephone service.
- Install radio telemetry distributed antennas throughout the facility.
- Use a badge identification system for building access.
- Install a CCTV surveillance system.
- Install an electronic security alarm system.
- Install rapid response and isolation features into HVAC systems.
- Use interior barriers to differentiate levels of security.
- Locate utility systems away from likely areas of potential attack.
- Install call buttons at key public contact areas.
- Install emergency and normal electric equipment at different locations.
- Avoid exposed structural elements.
- Reinforce foyer walls.
- Use architectural features to deny contact with exposed primary vertical load members.
- Isolate lobbies, mailrooms, loading docks, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- Elevate HVAC fresh-air intakes.
- Create "shelter-in-place" rooms or areas.
- Separate HVAC zones. Eliminate leaks and increase building air tightness.
- Install blast-resistant doors or steel doors with steel frames.
- Physically separate unsecured areas from the main building.
- Install HVAC exhausting and purging systems.
- Connect interior non-load bearing walls to structure with non-rigid connections.
- Use structural design techniques to resist progressive collapse.

Figure 5-4 Mitigation options for the third layer of defense



- Treat exterior shear walls as primary structures.
- Orient glazing perpendicular to the primary façade facing uncontrolled vehicle approaches.
- Use reinforced concrete wall systems in lieu of masonry or curtain walls.
- Ensure active fire system is protected from single-point failure in case of a blast event.
- Install a Backup Control Center (BCC).
- Avoid eaves and overhangs or harden to withstand blast effects.
- Establish ground floor elevation 4 feet above grade.
- Avoid re-entrant corners on the building exterior.

Figure 5-4 Mitigation options for the third layer of defense (continued)

WORKSHEET 5-1: PRELIMINARY MITIGATION OPTIONS

Prioritized Observations	Blast Regulatory Measures	CBR Regulatory Measures	Blast Repair and Strengthening of Existing Structures	CBR Repair and Strengthening of Existing Structures	Blast Protection and Control Measures	CBR Protection and Control Measures
Observation 1						
Observation 2						
Observation 3						
Observation 4						
Observation 5						
Observation 6						
Observation 7						
Observation 8						

Worksheet 5-1 will help to identify your preliminary mitigation options.

After you have prioritized your observations/vulnerabilities (Task 4.3), proceed to rank them for impact during blast and CBR events. Using the first part of the Worksheet (Prioritized Observations) indicate if these observations merit a regulatory, rehabilitation, and/or protective measure and if they directed at blast or CBR.

Using the second (Preliminary Mitigation Options for Blast) and third (Preliminary Mitigation Options for CBR) parts of the Worksheet, determine mitigation options that address the main concerns included in your observations and provided parameters.

Preliminary Mitigation Options for Blast	
Mitigation 1	
Mitigation 2	
Mitigation 3	
Mitigation 4	

Preliminary Mitigation Options for CBR	
Mitigation 5	
Mitigation 6	
Mitigation 7	
Mitigation 8	

WORKSHEET 5-2: PRELIMINARY MITIGATION OPTIONS

Worksheet 5-2 will help you to identify a short list of mitigation options. Bring forward preliminary mitigation options from Worksheet 5-1 and review them against the list of criteria provided in the upper part of the worksheet. The selected criteria are described in Task 5.2. Mark with a plus "+" or a minus "-" as to whether your preliminary mitigation options have positive or negative impact. The lower portion of the worksheet is reserved for writing a short list of options as a result of the former exercise.

	Available Political Support	Community Acceptance	Cost	Benefit	Available Financial Resources	Legal Authority	Adverse Effects on the Already Built Environment	Adversely Affected Population	Environmental Impact	Technical Capacity	Funding for Maintenance and Operations	Ease and Speed of Implementation	Timeframe and Urgency	Short-Term Solutions/Benefits	Long-Term Solutions/Benefits	Others
Mitigation 1																
Mitigation 2																
Mitigation 3																
Mitigation 4																
Mitigation 5																
Mitigation 6																
Mitigation 7																
Short List of Mitigation Options for Blast																
Option 1																
Option 2																
Option 3																
Short List of Mitigation Options for CBR																
Option 1																

APPENDIX A: BUILDING VULNERABILITY ASSESSMENT CHECKLIST

The Building Vulnerability Assessment Checklist is based on the checklist developed by the Department of Veterans Affairs (VA) and is part of FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. This Checklist will help you to prepare your Threat Assessment because it allows a consistent security evaluation of designs at various levels. The Checklist can be used as a screening tool for preliminary design vulnerability assessment and supports the preparation of all steps in this How-To Guide.

The Checklist is organized into 13 sections: 1) site, 2) architectural, 3) structural systems, 4) building envelope, 5) utility systems, 6) mechanical systems, 7) plumbing and gas systems, 8) electrical systems, 9) fire alam sysems, 10) communications and information technology (IT) systems, 11) equipment operations and maintenance, 12) security systems, and 13) security master plan. To conduct a vulnerability assessment of a building or preliminary design, each section of the Checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area. Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. If assessing an existing building, vulnerabilities can also be documented with photographs, if possible. The results of the 13 assessments should be integrated into a master vulnerability assessment and provide a basis for determining vulnerability ratings during the assessment process.

Section	Vulnerability Question	Guidance	Observations
1	**Site**		
1.1	**What major structures surround the facility (site or building(s))?** **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)?** **What are the adjacent land uses immediately outside the perimeter of this facility (site or building(s))?**	**Critical infrastructure to consider includes:** **Telecommunications infrastructure** Facilities for broadcast TV, cable TV; cellular networks; newspaper offices, production, and distribution; radio stations; satellite base stations; telephone trunking and switching stations, including critical cable routes and major rights-of-way **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	

Section	Vulnerability Question	Guidance	Observations
1	Site		
	Do future development plans change these land uses outside the facility (site or building (s)) perimeter? Although this question bridges threat and vulnerability, the threat is the manmade hazard that can occur (likelihood and impact) and the vulnerability is the proximity of the hazard to the building(s) being assessed. Thus, a chemical plant release may be a threat/hazard, but vulnerability changes if the plant is 1 mile upwind for the prevailing winds versus 10 miles away and downwind. Similarly, a terrorist attack upon an adjacent building may impact the building(s) being assessed. The Murrah Federal Building in Oklahoma City was not the only building to have severe damage caused by the explosion of the Ryder rental truck bomb.	**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 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 Center (EMCs), law enforcement facilities	

Section	Vulnerability Question	Guidance	Observations
1	**Site**		
		The following are not critical infrastructure, but have potential collateral damage 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 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*	
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*	

Section	Vulnerability Question	Guidance	Observations
1	**Site**		
1.3	**In dense, urban areas, does curb lane parking allow uncontrolled vehicles to park unacceptably close to a building in public rights-of-way?**	Where distance from the building to the nearest curb provides insufficient setback, restrict parking in the curb lane. For typical city streets, this may require negotiating to close the curb lane. Setback is common terminology for the distance between a building and its associated roadway or parking. It is analogous to stand-off between a vehicle bomb and the building. The benefit per foot of increased stand-off between a potential vehicle bomb and a building is very high when close to a building and decreases rapidly as the distance increases. Note that the July 1, 1994, Americans with Disabilities Act Standards for Accessible Design states that required handicapped parking shall be located on the shortest accessible route of travel from adjacent parking to an accessible entrance. Reference: *GSA PBS-P100*	
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*	
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*	
1.6	**Is vehicle traffic separated from pedestrian traffic on the site?**	Pedestrian access should not be endangered by car traffic. Pedestrian access, especially from public transportation, should not cross vehicle traffic if possible. References: *GSA PBS-P100 and FEMA 386-7*	
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*	

Section	Vulnerability Question	Guidance	Observations
1	**Site**		
1.8	**Is there space for inspection at the curb line or outside the protected perimeter?** **What is the minimum distance from the inspection location to the building?**	Design features for the vehicular inspection point include: vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and prevent tailgating. If screening space cannot be provided, consider other design features such as: hardening and alternative location for vehicle search/inspection. Reference: *GSA PBS-P100*	
1.9	**Is there any potential access to the site or building through utility paths or water runoff?**	Eliminate potential site access through utility tunnels, corridors, manholes, stormwater runoff culverts, etc. Ensure covers to these access points are secured. Reference: *USAF Installation Force Protection Guide*	
1.10	**What are the existing types of vehicle anti-ram devices for the site or building?** **Are these devices at the property boundary or at the building?**	Passive barriers include bollards, walls, hardened fences (steel cable interlaced), trenches, ponds/basins, concrete planters, street furniture, plantings, trees, sculptures, and fountains. Active barriers include pop-up bollards, swing arm gates, and rotating plates and drums, etc. Reference: *GSA PBS-P100*	
1.11	**What is the anti-ram buffer zone stand-off distance from the building to unscreened vehicles or parking?**	If the recommended distance for the postulated threat is not available, consider reducing the stand-off required through structural hardening or manufacturing additional stand-off through barriers and parking restrictions. Also, consider relocation of vulnerable functions within the building, or to a more hazard-resistant building. More stand-off should be used for unscreened vehicles than for screened vehicles that have been searched. Reference: *GSA PBS-P100*	
1.12	**Are perimeter barriers capable of stopping vehicles?** **Will the vehicle barriers at the perimeter and building maintain access for emergency responders, including large fire apparatus?**	Anti-ram protection may be provided by adequately designed: bollards, street furniture, sculpture, landscaping, walls, and fences. The anti-ram protection must be able to stop the threat vehicle size (weight) at the speed attainable by that vehicle at impact. If the anti-ram protection cannot absorb the desired kinetic energy, consider adding speed controls (serpentines or speed bumps) to limit the speed at impact. If the resultant speed is still too great, the anti-ram protection should be improved. References: *Military Handbook 1013/14 and GSA PBS P-100*	

Section	Vulnerability Question	Guidance	Observat ions
1	**Site**		
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*	
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*	
1.15	**Is there a minimum setback distance between the building and parked vehicles?**	Adjacent public parking should be directed to more distant or better-protected areas, segregated from employee parking and away from the building. Some publications use the term setback in lieu of the term stand-off. Reference: *GSA PBS-P100*	
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*	
1.17	**Do standalone, aboveground parking garages provide adequate visibility across as well as into and out of the parking garage?**	Pedestrian paths should be planned to concentrate activity to the extent possible. Limiting vehicular entry/exits to a minimum number of locations is beneficial. Stair tower and elevator lobby design should be as open as code permits. Stair and/or elevator waiting areas should be as open to the exterior and/or the parking areas as possible and well lighted. Impact-resistant, laminated glass for stair towers and elevators is a way to provide visual openness. Potential hiding places below stairs should be closed off; nooks and crannies should be avoided, and dead-end parking areas should be eliminated. Reference: *GSA PBS-P100*	
1.18	**Are garage or service area entrances for employee-permitted vehicles protected by suitable anti-ram devices?** **Coordinate this protection with other anti-ram devices, such as on the perimeter or property boundary to avoid duplication of arresting capability.**	Control internal building parking, underground parking garages, and access to service areas and loading docks in this manner with proper access control, or eliminate the parking altogether. The anti-ram device must be capable of arresting a vehicle of the designated threat size at the speed attainable at the location.	

Section	Vulnerability Question	Guidance	Observations
1	**Site**		
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*	
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*	
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 or vehicles outside normal circulation routes or attempting to approach the building unobserved. Reference: *USAF Installation Force Protection Guide*	
1.22	**Do signs provide control of vehicles and people?**	The signage should be simple and have the necessary level of clarity. However, signs that identify sensitive areas should generally not be provided. Reference: *GSA PBS-P100*	
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*	

Section	Vulnerability Question	Guidance	Observations
2	**Architectural**		
2.1	**Does the site and architectural design incorporate strategies from a Crime Prevention Through Environmental Design (CPTED) perspective?**	**The focus of CPTED is on creating defensible space by employing:** **1. Natural access controls:** – Design streets, sidewalks, and building entrances to clearly indicate public routes and direct people away from private/restricted areas – Discourage access to private areas with structural elements and limit access (no cut-through streets) – Loading zones should be separate from public parking **2. Natural surveillance:** – Design that maximizes visibility of people, parking areas, and building entrances; doors and windows that look out on to streets and parking areas – Shrubbery under 2 feet in height for visibility – Lower branches of existing trees kept at least 10 feet off the ground – Pedestrian-friendly sidewalks and streets to control pedestrian and vehicle circulation – Adequate nighttime lighting, especially at exterior doorways **3. Territorial reinforcement:** – Design that defines property lines – Design that distinguishes private/restricted spaces from public spaces using separation, landscape plantings; pavement designs (pathway and roadway placement); gateway treatments at lobbies, corridors, and door placement; walls, barriers, signage, lighting, and "CPTED" fences – "Traffic-calming" devices for vehicle speed control **4. Target hardening:** – Prohibit entry or access: window locks, deadbolts for doors, interior door hinges – Access control (building and employee/visitor parking) and intrusion detection systems **5. Closed circuit television cameras:** – Prevent crime and influence positive behavior, while enhancing the intended uses of space. In other words, design that eliminates or reduces criminal behavior and at the same time encourages people to "keep an eye out" for each other. References: *GSA PBS-P100 and FEMA 386-7*	

Section	Vulnerability Question	Guidance	Observations
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*	
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*	
2.4	**Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?**	The size of the trash receptacles and mailbox openings should be restricted to prohibit insertion of packages. Street furniture, such as newspaper vending machines, should be kept sufficient distance (10 meters or 33 feet) from the building, or brought inside to a secure area. References: *USAF Installation Force Protection Guide and DoD UCF 4-010-01*	
2.5	**Do entrances avoid significant queuing?**	If queuing will occur within the building footprint, the area should be enclosed in blast-resistant construction. If queuing is expected outside the building, a rain cover should be provided. For manpower and equipment requirements, collocate or combine staff and visitor entrances. Reference: *GSA PBS-P100*	
2.6	**Does security screening cover all public and private areas?** **Are public and private activities separated?** **Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?**	Retail activities should be prohibited in non-secured areas. However, the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting buildings. Consider separating entryways, controlling access, hardening shared partitions, and special security operational countermeasures. References: *GSA PBS-P100 and FEMA 386-7*	

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*	
2.8	**Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?**	Finishes and signage should be designed for visual simplicity. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
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*	
2.11	**Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?**	Consider for exterior entrances to the building or to access critical areas within the building if explosive blast hazard must be mitigated. Reference: *U.S. Army TM 5-853*	
2.12	**Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?**	If the postulated threat in designing entrance access control includes rifles, pistols, or shotguns, then the screening area should have bullet-resistance to protect security personnel and uninvolved bystanders. Glass, if present, should also be bullet-resistant. Reference: *GSA PBS-P100*	
2.13	**Do circulation routes have unobstructed views of people approaching controlled access points?**	This applies to building entrances and to critical areas within the building. References: *USAF Installation Force Protection Guide and DoD UFC 4-010-01*	

Section	Vulnerability Question	Guidance	Observations
2	**Architectural**		
2.14	**Is roof access limited to authorized personnel by means of locking mechanisms?**	References: *GSA PBS-P100 and CDC/NIOSH, Pub 2002-139*	
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 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*	
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*	
2.17	**Is high visitor activity away from critical assets?**	High-risk activities should also be separated from low-risk activities. Also, visitor activities should be separated from daily activities. Reference: *USAF Installation Force Protection Guide*	
2.18	**Are critical assets located in spaces that are occupied 24 hours per day?** **Are assets located in areas where they are visible to more than one person?**	Reference: *USAF Installation Force Protection Guide*	

Section	Vulnerability Question	Guidance	Observations
2 Architectural			
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*	
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*	
2.21	**Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?**	Screening of all deliveries to the building, including U.S. mail, commercial package delivery services, delivery of office supplies, etc. Reference: *GSA PBS-P100*	
2.22	**Are areas of refuge identified, with special consideration given to egress?**	Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards. Reference: *FEMA 386-7*	
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 areas other than lobbies, parking, or loading docks. 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. References: *GSA PBS-P100 and CDC/NIOSH, Pub 2002-139*	

Section	Vulnerability Question	Guidance	Observations
2	**Architectural**		
2.24	**Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?**	Egress pathways should be hardened and discharge into safe areas. Reference: *FEMA 386-7*	
2.25	**Do interior barriers differentiate level of security within a building?**	Reference: *USAF Installation Force Protection Guide*	
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 does not take out all capability – both the regular systems and their backups. Reference: *FEMA 386-7*	
2.27	**Is interior glazing near high-risk areas minimized?** **Is interior glazing in other areas shatter-resistant?**	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. Reference: *GSA PBS-P100*	
2.28	**Are ceiling and lighting systems designed to remain in place during hazard events?**	When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and non-structural building components under loads not considered in standard building codes. It has been shown that connection criteria for these systems in high seismic activity areas resulted in much less falling debris that could injure building occupants. Mount all overhead utilities and other fixtures weighing 14 kilograms (31 pounds) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This standard does not preclude the need to design equipment mountings for forces required by other criteria, such as seismic standards. Reference: *DoD UCF 4-101-01*	

Section	Vulnerability Question	Guidance	Observations
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 un-reinforced. A rapid screening process developed by FEMA for assessing structural hazards identifies the following types of construction with a structural score ranging from 1.0 to 8.5. A higher score indicates a greater capacity to sustain load reversals. Wood buildings of all types - 4.5 to 8.5 Steel moment-resisting frames - 3.5 to 4.5 Braced steel frames - 2.5 to 3.0 Light metal buildings - 5.5 to 6.5 Steel frames with cast-in-place concrete shear walls - 3.5 to 4.5 Steel frames with unreinforced masonry infill walls - 1.5 to 3.0 Concrete moment-resisting frames - 2.0 to 4.0 Concrete shear wall buildings - 3.0 to 4.0 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*	
3.2	**Do the reinforced concrete structures contain symmetric steel reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams, and girders that may be subjected to rebound, uplift, and suction pressures?**	Reference: *GSA PBS-P100*	

Section	Vulnerability Question	Guidance	Observations
3	**Structural Systems**		
	Do the lap splices fully develop the capacity of the reinforcement? **Are lap splices and other discontinuities staggered?** **Do the connections possess ductile details?** **Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?**		
3.3	**Are the steel frame connections moment connections?** **Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system?** **What are the floor-to-floor heights?**	A practical upper level for column spacing is generally 30 feet. Unless there is an overriding architectural requirement, a practical limit for floor-to-floor heights is generally less than or equal to 16 feet. Reference: *GSA PBS-P100*	
3.4	**Are critical elements vulnerable to failure?**	The priority for upgrades should be based on the relative importance of structural or non-structural elements that are essential to mitigating the extent of collapse and minimizing injury and damage. Primary Structural Elements provide the essential parts of the building's resistance to catastrophic blast loads and progressive collapse. These include columns, girders, roof beams, and the main lateral resistance system. Secondary Structural Elements consist of all other load-bearing members, such as floor beams, slabs, etc. Primary Non-Structural Elements consist of elements (including their attachments) that are essential for life safety systems or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units. Secondary Non-Structural Elements consist of all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures. Reference: *GSA PBS-P100*	

Section	Vulnerability Question	Guidance	Observations
3	**Structural Systems**		
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 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?** **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?**	Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted. Reference: *GSA PBS-P100*	

Section	Vulnerability Question	Guidance	Observations
3	**Structural Systems**		
	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?**		
3.7	**Are there adequate redundant load paths in the structure?**	Special consideration should be given to materials that have inherent ductility and that are better able to respond to load reversals, such as cast in place reinforced concrete, reinforced masonry, and steel construction. Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Primary vertical load carrying members should be protected where parking is inside a facility and the building superstructure is supported by the parking structure. Reference: *GSA PBS-P100*	
3.8	**Are there transfer girders supported by columns within unscreened public spaces or at the exterior of the building?**	Transfer girders allow discontinuities in columns between the roof and foundation. This design has inherent difficulty in transferring load to redundant paths upon loss of a column or the girder. Transfer beams and girders that, if lost, may cause progressive collapse are highly discouraged. Reference: *GSA PBS-P100*	
3.9	**What is the grouting and reinforcement of masonry (brick and/or concrete masonry unit (CMU)) exterior walls?**	Avoid unreinforced masonry exterior walls. Reinforcement can run the range of light to heavy, depending upon the stand-off distance available and postulated design threat. Reference: *GSA PBS-P100* recommends fully grouted and reinforced CMU construction where CMU is selected.	

Section	Vulnerability Question	Guidance	Observations
3	**Structural Systems**		
		Reference: *DoD Minimum Antiterrorism Standards for Buildings* states "Unreinforced masonry walls are prohibited for the exterior walls of new buildings. A minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1200 mm (48 in) will be provided. For existing buildings, implement mitigating measures to provide an equivalent level of protection." [This is light reinforcement and based upon the recommended stand-off distance for the situation.]	
3.10	**Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?**	Design the floor of the loading dock for blast resistance if the area below is occupied or contains critical utilities. Reference: *GSA PBS-P100*	
3.11	**Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?**	Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment- resistant. Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside. Reference: *GSA PBS-P100*	
4	**Building Envelope**		
4.1	**What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?**	The performance of the façade varies to a great extent on the materials. Different construction includes brick or stone with block backup, steel stud walls, precast panels, or curtain wall with glass, stone, or metal panel elements. Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls should be considered primary structures and should resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration should be given to construction types that reduce the potential for injury. Reference: *GSA PBS-P100*	

Section	Vulnerability Question	Guidance	Observations
4	**Building Envelope**		
4.2	**Is there less than a 40 percent fenestration opening 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). Reference: *GSA PBS-P100*	
4.3	**Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected?** **Are the walls capable of withstanding the dynamic reactions from the windows?** **Will the anchorage remain attached to the walls of the building during an explosive event without failure?** **Is the façade connected to backup block or to the structural frame?** **Are non-bearing masonry walls reinforced?**	Government produced and sponsored computer programs coupled with test data and recognized dynamic structural analysis techniques may be used to determine whether the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants. A breakage probability no higher than 750 breaks per 1,000 may be used when calculating loads to frames and anchorage. The intent is to ensure the building envelope provides relatively equal protection against the postulated explosive threat for the walls and window systems for the safety of the occupants, especially in rooms with exterior walls. Reference: *GSA PBS-P100*	
4.4	**Does the building contain ballistic glazing?**	Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material.	

Section	Vulnerability Question	Guidance	Observations
4	**Building Envelope**		
	Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing? **Does the building contain security-glazing?** **Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material?** **Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?**	If windows are upgraded to bullet-resistant, burglar-resistant, or forced entry-resistant, ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern. Reference: *GSA PBS-P100*	
4.5	**Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?**	n-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures. These non-window openings should also be as secure as the rest of the building envelope against forced entry. Reference: *GSA PBS-P100*	
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*	
5.2	**Are there multiple entry points for the water supply?**	If the building or site has only one source of water entering at one location, the entry point should be secure. Reference: *GSA PBS-P100*	
5.3	**Is the incoming water supply in a secure location?**	Ensure that only authorized personnel have access to the water supply and its components. Reference: *FEMA 386-7*	
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 the Department of Veterans Affairs Facilities.*	

Section	Vulnerability Question	Guidance	Observations
5	**Utility Systems**		
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*	
5.6	**Is the fire suppression system adequate, code-compliant, and protected (secure location)?**	Standpipes, water supply control valves, and other system components should be secure or supervised. Reference: *FEMA 386-7*	
5.7	**Do the sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation?** **Are the sprinkler and standpipe connections adequate and redundant?** **Are there fire hydrant and water supply connections near the sprinkler/standpipe connections?**	The incoming fire protection water line should be encased, buried, or located 50 feet from high-risk areas. The interior mains should be looped and sectionalized. Reference: *GSA PBS-P100*	
5.8	**Are there redundant fire water pumps (e.g., one electric, one diesel)?** **Are the pumps located apart from each other?**	Collocating fire water pumps puts them at risk for a single incident to disable the fire suppression system. References: *GSA PBS-P100 and FEMA 386-7*	
5.9	**Are sewer systems accessible?** **Are they protected or secured?**	Sanitary and stormwater sewers should be protected from unauthorized access. The main concerns are backup or flooding into the building, causing a health risk, shorting out electrical equipment, and loss of building use. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
5.10	**What fuel supplies do the building rely upon for critical operation?**	Typically, natural gas, propane, or fuel oil are required for continued operation. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
5	**Utility Systems**		
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*	
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*	
5.13	**Are there alternate sources of fuel?** **Can alternate fuels be used?**	Critical functions may be served by alternate methods if normal fuel supply is interrupted. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
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*	
5.16	**How many service entry points does the site or building have for electricity?**	Electrical supply at one location creates a vulnerable situation unless an alternate source is available. Ensure disconnecting requirements according to NFPA 70 (National Fire Protection Association, National Electric Code) are met for multiple service entrances. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
5.17	**Is the incoming electric service to the building secure?**	Typically, the service entrance is a locked room, inaccessible to the public. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
5	**Utility Systems**		
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*	
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*	
5.20	**Are there multiple or redundant locations for the telephone and communications service?**	Secure locations of communications wiring entry to the site or building are required. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
5.22	**Are utility lifelines aboveground, underground, or direct buried?**	Utility lifelines (water, power, communications, etc.) can be protected by concealing, burying, or encasing. References: *GSA PBS-P100 and FEMA 386-7*	

Section	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 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 this document, 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 concer n during an outdoor release, especially if exhaust fans are not in continuous operation, due to wind effects and chimney effects (air movement due to differential temperature).	
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. References: *GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959*	
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*	
6.4	**What are the types of air filtration? Include the efficiency and number of filter modules for**	MERV – Minimum Efficiency Reporting Value HEPA – High Efficiency Particulate Air	

Section	Vulnerability Question	Guidance	Observations
6 Mechanical Systems (HVAC and CBR)			
	each of the main air handling systems? **Is there any collective protection for chemical, biological, and radiological contamination designed into the building?**	Activated charcoal for gases Ultraviolet C for biologicals Consider mix of approaches for optimum protection and cost-effectiveness. Reference: *CDC/NIOSH Pub 2002-139*	
6.5	**Is there space for larger filter assemblies on critical air handling systems?**	Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. However, upgraded filtration may have negative effects upon the overall air handling system operation, such as increased pressure drop. Reference: *CDC/NIOSH Pub 2002-139*	
6.6	**Are there µprovisions for air monitors or sensors for chemical or biological agents?**	Duct mounted sensors are usuallly found in limited cases in laboratory areas. Sensors generally have a limited spectrum of high reliability and are costly. Many different technologies are undergoing research to provide capability. Reference: *CDC/NIOSH Pub 2002-139*	
6.7	**By what method are air intakes and exhausts closed when not operational?**	Motorized (low-leakage, fast-acting) dampers are the preferred method for closure with fail-safe to the closed position so as to support in-place sheltering. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.8	**How are air handling systems zoned?** **What areas and functions do each of the primary air handling systems serve?**	Understanding the critical areas of the building that must continue functioning focuses security and hazard mitigation measures. Applying HVAC zones that isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building HVAC zones and maintaining negative pressure within these areas will contain CBR releases. Identify common return systems that service more than one zone, effectively making a large single zone. Conversely, emergency egress routes should receive positive pressurization to ensure contamination does not hinder egress. Consider filtering of the pressurization air. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.9	**Are there large central air handling units or are there multiple units serving separate zones?**	Independent units can continue to operate if damage occurs to limited areas of the building. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
6 Mechanical Systems (HVAC and CBR)			
6.10	**Are there any redundancies in the air handling system?** **Can critical areas be served from other units if a major system is disabled?**	Redundancy reduces the security measures required compared to a non-redundant situation. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
6.11	**Is the air supply to critical areas compartmentalized?** **Similarly, are the critical areas or the building as a whole, considered tight with little or no leakage?**	During chemical, biological, and radiological situations, the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects. Smoke testing of the air supply to critical areas may be necessary. Reference: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.12	**Are supply, return, and exhaust air systems for critical areas secure?** **Are all supply and return ducts completely connected to their grilles and registers and secure?** **Is the return air not ducted?**	The air systems to critical areas should be inaccessible to the public, especially if the ductwork runs through the public areas of the building. It is also more secure to have a ducted air handling system versus sharing hallways and plenums above drop ceilings for return air. Non-ducted systems provide greater opportunity for introducing contaminants. Reference: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.13	**What is the method of temperature and humidity control?** **Is it localized or centralized?**	Central systems can range from monitoring only to full control. Local control may be available to override central operation. Of greatest concern are systems needed before, during, and after an incident that may be unavailable due to temperature and humidity exceeding operational limits (e.g., main telephone switch room). Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
6.14	**Where are the building automation control centers and cabinets located?**	Access to any component of the building automation and control system could compromise the functioning of the system, increasing vulnerability to a hazard or precluding their proper operation during a hazard incident.	

Section	Vulnerability Question	Guidance	Observations
6	**Mechanical Systems (HVAC and CBR)**		
	Are they in secure areas? **How is the control wiring routed?**	The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack. References: *FEMA 386-7, DOC CIAO Vulnerability Assessment Framework 1.1 and LBNL Pub 51959*	
6.15	**Does the control of air handling systems support plans for sheltering in place or other protective approach?**	The micro-meteorological effects of buildings and terrain can alter travel and duration of chemical agents and hazardous material releases. Shielding in the form of sheltering in place can protect people and property from harmful effects. To support in-place sheltering, the air handling systems require the ability for authorized personnel to rapidly turn off all systems. However, if the system is properly filtered, then keeping the system operating will provide protection as long as the air handling system does not distribute an internal release to other portions of the building. Reference: *CDC/NIOSH Pub 2002-139*	
6.16	**Are there any smoke evacuation systems installed?** **Does it have purge capability?**	For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high-risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk on internal events, such as lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants. References: *GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959*	
6.17	**Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)**	Roof-mounted equipment should be kept away from the building perimeter. Reference: *U.S. Army TM 5-853*	
6.18	**Are fire dampers installed at all fire barriers?** **Are all dampers functional and seal well when closed?**	All dampers (fire, smoke, outdoor air, return air, bypass) must be functional for proper protection within the building during an incident. Reference: *CDC/NIOSH Pub 2002-139*	
6.19	**Do fire walls and fire doors maintain their integrity?**	The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal, by zone ducting, fire walls, fire stops, and fire doors) provides energy conservation benefits and functional benefits during a CBR incident. Reference: *LBNL Pub 51959*	

Section	Vulnerability Question	Guidance	Observations
6	**Mechanical Systems (HVAC and CBR)**		
6.20	**Do elevators have recall capability and elevator emergency message capability?**	Although a life-safety code and fire response requirement, the control of elevators also has benefit during a CBR incident. The elevators generate a piston effect, causing pressure differentials in the elevator shaft and associated floors that can force contamination to flow up or down. Reference: *LBNL Pub 51959*	
6.21	**Is access to building information restricted?**	Information on building operations, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.22	**Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure CBR equipment is functional?**	Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired. The HVAC system can be operated in different ways, depending upon an external or internal release and where in the building an internal release occurs. Thus maintenance and security staff must have the training to properly operate the HVAC system under different circumstances, even if the procedure is to turn off all air movement equipment. Reference: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
7	**Plumbing and Gas Systems**		
7.1	**What is the method of water distribution?**	Central shaft locations for piping are more vulnerable than multiple riser locations. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
7.2	**What is the method of gas distribution? (heating, cooking, medical, process)**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
7.3	**Is there redundancy to the main piping distribution?**	Looping of piping and use of section valves provide redundancies in the event sections of the system are damaged. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
7	**Plumbing and Gas Systems**		
7.4	**What is the method of heating domestic water?** **What fuel(s) is used?**	Single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types. Domestic hot water availability is an operational concern for many building occupancies. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
7.5	**Where are gas storage tanks located? (heating, cooking, medical, process)** **How are they piped to the distribution system? (above or below ground)**	The concern is that the tanks and piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher-risk area. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
7.6	**Are there reserve supplies of critical gases?**	Localized gas cylinders could be available in the event of damage to the central tank system. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
8.2	**What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
8.3	**How are the electrical rooms secured and where are they located relative to other higher-risk areas, starting with the main electrical distribution room at the service entrance?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
8	**Electrical Systems**		
8.4	**Are critical electrical systems collocated with other building systems?** **Are critical electrical systems located in areas outside of secured electrical areas?** **Is security system wiring located separately from electrical and other service systems?**	Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
8.5	**How are electrical distribution panels serving branch circuits secured or are they in secure locations?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
8.7	**How is the primary electrical system wiring distributed?** **Is it collocated with other major utilities?** **Is there redundancy of distribution to critical areas?**	Central utility shafts may be subject to damage, especially if there is only one for the building. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
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*	
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*	
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*	
9.4	**Do key fire alarm system components have fire- and blast-resistant separation?**	This is especially necessary for the fire command center or fire alarm control center. The concern is to similarly protect critical components as described in Items 2.19, 5.7, and 10.3.	
9.5	**Is there redundant off-premises fire alarm reporting?**	Fire alarms can ring at a fire station, at an intermediary alarm monitoring center, or autodial someone else. See Items 5.21 and 10.5.	
10	**Communications and IT Systems**		
10.1	**Where is the main telephone distribution room and where is it in relation to higher-risk areas?** **Is the main telephone distribution room secure?**	One can expect to find voice, data, signal, and alarm systems to be routed through the main telephone distribution room. Reference: *FEMA 386-7*	

Section	Vulnerability Question	Guidance	Observations
10	**Communications and IT Systems**		
10.2	**Does the telephone system have an uninterruptible power supply (UPS)?** **What is its type, power rating, and operational duration under load, and location? (battery, on-line, filtered)**	Many telephone systems are now computerized and need a UPS to ensure reliability during power fluctuations. The UPS is also needed to await any emergency power coming on line or allow orderly shutdown. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.3	**Where are communication systems wiring closets located? (voice, data, signal, alarm)** **Are they collocated with other utilities?** **Are they in secure areas?**	Concern is to have separation distance from other utilities and higher-risk areas to avoid collateral damage. Security approaches on the closets include door alarms, closed circuit television, swipe cards, or other logging notifications to ensure only authorized personnel have access to these closets. Reference: *FEMA 386-7*	
10.4	**How is the communications system wiring distributed? (secure chases and risers, accessible public areas)**	The intent is to prevent tampering with the systems. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
10.6	**Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure?** **Where are the secondary and/or intermediate distribution facilities and are they secure?**	Concern is collateral damage from manmade hazards and redundancy of critical functions. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.7	**What type and where are the Wide Area Network (WAN) connections?**	Critical facilities should have two Minimum-Points-of-Presence(MPOPs) where the telephone company's outside cable terminates inside the building. It is functionally a service entrance connection that demarcates where the telephone company's property stops and the building owner's property begins. The MPOPs should not be collocated and they should connect to different telephone company central offices so that the loss of one cable or central office does not reduce capability. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
10	**Communications and IT Systems**		
10.8	**What are the type, power rating, and location of the uninterruptible power supply?** (battery, on-line, filtered) **Are the UPS also connected to emergency power?**	Consider that UPS should be found at all computerized points from the main distribution facility to individual data closets and at critical personal computers/terminals. Critical LAN sections should also be on backup power. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.9	**What type of Local Area Network (LAN) cabling and physical topology is used?** (Category (Cat) 5, Gigabit Ethernet, Ethernet, Token Ring)	The physical topology of a network is the way in which the cables and computers are connected to each other. The main types of physical topologies are: Bus (single radial where any damage on the bus affects the whole system, but especially all portions downstream) Star (several computes are connected to a hub and many hubs can be in the network – the hubs can be critical nodes, but the other hubs continue to function if one fails) Ring (a bus with a continuous connection - least used, but can tolerate some damage because if the ring fails at a single point it can be rerouted much like a looped electric or water system) The configuration and the availability of surplus cable or spare capacity on individual cables can reduce vulnerability to hazard incidents. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
10.10	**For installed radio/wireless systems, what are their types and where are they located?** (radio frequency (RF), high frequency (HF), very high frequency (VHF), medium wave (MW))	Depending upon the function of the wireless system, it could be susceptible to accidental or intended jamming or collateral damage. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
10.11	**Do the Information Technology (IT - computer) systems meet requirements of confidentiality, integrity, and availability?**	Ensure access to terminals and equipment for authorized personnel only and ensure system up-time to meet operational needs. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	

Section	Vulnerability Question	Guidance	Observations
10	**Communications and IT Systems**		
10.12	**Where is the disaster recovery/ mirroring site?**	A site with suitable equipment that allows continuation of operations or that mirrors (operates in parallel to) the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.13	**Where is the backup tape/file storage site and what is the type of safe environment?** (safe, vault, underground) **Is there redundant refrigeration in the site?**	If equipment is lost, data are most likely lost, too. Backups are needed to continue operations at the disaster recovery site or when equipment can be delivered and installed. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.14	**Are there any satellite communications (SATCOM) links?** (location, power, UPS, emergency power, spare capacity/capability)	SATCOM links can serve as redundant communications for voice and data if configured to support required capability after a hazard incident. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.15	**Is there a mass notification system that reaches all building occupants?** (public address, pager, cell phone, computer override, etc.) **Will one or more of these systems be operational under hazard conditions?** (UPS, emergency power)	Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident if there is redundancy and power. Reference: *DoD UFC 4-010-01*	
10.16	**Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass notification, etc.? (emergency operations, security, fire alarms, building automation)** **Do the alternate locations also have access to backup systems, including emergency power?**	Reference: *GSA PBS-P100*	

Section	Vulnerability Question	Guidance	Observations
11	**Equipment Operations and Maintenance**		
11.1	**Are there composite drawings indicating location and capacities of major systems and are they current?** (electrical, mechanical, and fire protection; and date of last update) **Do updated operations and maintenance (O&M) manuals exist?**	Within critical infrastructure protection at the building level, the current configuration and capacity of all critical systems must be understood to ensure they meet emergency needs. Manuals must also be current to ensure operations and maintenance keeps these systems properly functioning. The system must function during an emergency unless directly affected by the hazard incident. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
11.2	**Have critical air systems been rebalanced?** **If so, when and how often?**	Although the system may function, it must be tested periodically to ensure it is performing as designed. Balancing is also critical after initial construction to set equipment to proper performance per the design. Rebalancing may only occur during renovation. Reference: *CDC/NIOSH Pub 2002-139*	
11.3	**Is air pressurization monitored regularly?**	Some areas require positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation. Measuring pressure drop across filters is an indication when filters should be changed, but also may indicate that low pressures are developing downstream and could result in loss of expected protection. Reference: *CDC/NIOSH Pub 2002-139*	
11.4	**Does the building have a policy or procedure for periodic recommissioning of major Mechanical/Electrical/Plumbing (M/E/P) systems?**	Recommissioning involves testing and balancing of systems to ascertain their capability to perform as described. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
11.5	**Is there an adequate O&M program, including training of facilities management staff?**	If O&M of critical systems is done with in-house personnel, management must know what needs to be done and the workforce must have the necessary training to ensure systems reliability. Reference: *CDC/NIOSH Pub 2002-139*	
11.6	**What maintenance and service agreements exist for M/E/P systems?**	When an in-house facility maintenance work force does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
11	**Equipment Operations and Maintenance**		
11.7	**Are backup power systems periodically tested under load?**	Loading should be at or above maximum connected load to ensure available capacity and automatic sensors should be tested at least once per year. Periodically (once a year as a minimum) check the duration of capacity of backup systems by running them for the expected emergency duration or estimating operational duration through fuel consumption, water consumption, or voltage loss. Reference: *FEMA 386-7*	
11.8	**Is stairway and exit sign lighting operational?**	The maintenance program for stairway and exit sign lighting (all egress lighting) should ensure functioning under normal and emergency power conditions. Expect building codes to be updated as emergency egress lighting is moved from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured. Reference: *FEMA 386-7*	
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?** **Are they analog or digital by design?** **What are 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?**	Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost-effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design. 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*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
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*	
12.3	**What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
12.5	**Are intercom call boxes used in parking areas or along the building perimeter?**	See Item 12.4.	
12.6	**What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.7	**Who monitors the CCTV system?**	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
12.8	**What is the quality of video images both during the day and hours of darkness?** **Are infrared camera illuminators used?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
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*	
12.10	**What type of exterior Intrusion Detection System (IDS) sensors are used?** (electromagnetic; fiber optic; active infrared; bistatic microwave; seismic; photoelectric; ground; fence; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches)	Consider balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors, and review roof intrusion detection. Consider glass break sensors for windows up to scalable heights. Reference: *GSA PBS-P100*	
12.11	**Is a global positioning system (GPS) used to monitor vehicles and asset movements?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
Interior Security			
12.12	**Are black/white or color CCTV cameras used?** **Are they monitored and recorded 24 hours/7 days a week? By whom?** **Are they analog or digital by design?** **What are 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?**	See Item 12.1. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
12.13	**Are the cameras programmed to respond automatically to interior 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. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.14	**What type of camera housings are used and are they designed to protect against exposure or tampering?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.15	**Do the camera lenses used have the proper specifications, especially distance viewing and clarity?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.16	**What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.17	**Are the interior camera video images of good visual and recording quality?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.18	**Are the interior cameras supported by an uninterruptible power supply source, battery, or building emergency power?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.19	**What are the first costs and maintenance costs associated with the interior cameras?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.20	**What type of security access control system is used?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
	Are the devices used for physical security also used (integrated) with security computer networks (e.g., in place of or in combination with user ID and system passwords)?		
12.21	**What type of access control transmission media is used to transmit access control system signals (same as defined for CCTV cameras)?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.22	**What is the backup power supply source for the access control systems?** (battery, uninterruptible power supply)	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.23	**What access control system equipment is used?** **How old are the systems and what are the related first and maintenance service costs?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.24	**Are panic/duress alarm sensors used?** **Where are they located?** **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*	
12.25	**Are intercom call-boxes or a building intercom system used throughout the building?**	See Item 12.24.	
12.26	**Are magnetometers (metal detectors) and x-ray equipment used?** **At what locations within the building?**	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
12.27	**What type of interior IDS sensors are used: electromagnetic; fiber optic; active infrared-motion detector; photoelectric; glass break (vibration/ shock); single, double, and roll-up door magnetic contacts or switches?**	Consider magnetic reed switches for interior doors and openings. Reference: *GSA PBS-P100*	
12.28	**Are mechanical, electrical, gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms continuously locked, under electronic security, CCTV camera, and intrusion alarm systems surveillance?**	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
12.29	**What types of locking hardware are used throughout the building?** **Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes, and related hardware and software used?**	As a minimum, electric utility closets, mechanical rooms, and telephone closets should be secured. The mailroom should also be secured, allowing only authorized personnel into the area where mail is screened and sorted. Separate the public access area from the screening area for the postulated mailroom threats. All security locking arrangements on doors used for egress must comply with *NFPA 101, Life Safety Code.* Reference: *GSA PBS-P100*	
12.30	**Are any potentially hazardous chemicals, combustible, or toxic materials stored on site in non-secure and non-monitored areas?**	The storage, use, and handling locations should also be kept away from other activities. The concern is that an intruder need not bring the material into the building if it is already there and accessible. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.31	**What security controls are in place to handle the processing of mail and protect against potential biological, explosive, or other threatening exposures?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
12.32	**Is there a designated security control room and console in place to monitor security, fire alarm, and other building systems?** **Is there a backup control center designated and equipped?** **Is there off-site 24-hour monitoring of intrusion detection systems?**	Monitoring can be done at an off-site facility, at an on-site monitoring center during normal duty hours, or at a 24-hour on-site monitoring center. Reference: *GSA PBS-P100*	
12.33	**Is the security console and control room adequate in size and does it provide room for expansion?** **Does it have adequate environment controls (e.g., a/c, lighting, heating, air circulation, backup power)?** **Is it ergonomically designed?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.34	**Is the location of the security room in a secure area with limited, controlled, and restricted access controls in place?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.35	**What are the means by which facility and security personnel can communicate with one another (e.g., portable radio, pager, cell phone, personal data assistants (PDAs))?** **What problems have been experienced with these and other electronic security systems?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.36	**Is there a computerized security incident reporting system used to prepare reports and track security incident trends and patterns?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.37	**Does the current security force have access to a computerized guard tour system?**	This system allows for the systematic performance of guard patrols with validation indicators built in. The system notes stations/locations checked or missed, dates and times of such patrols, and who conducted them on what shifts. Management reports can be produced for recordkeeping and manpower analysis purposes. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
12.38	**Are vaults or safes in the building?** **Where are they located?**	Basic structural design requires an understanding of where heavy concentrations of floor loading may occur so as to strengthen the floor and structural framing to handle this downward load. Security design also needs this information to analyze how this concentrated load affects upward and downward loadings under blast conditions and its impact upon progressive collapse. Location is important because safes can be moved by blast so that they should be located away from people and away from exterior windows. Vaults, on the other hand, require construction above the building requirements with thick masonry walls and steel reinforcement. A vault can provide protection in many instances due to its robust construction. Safes and vaults may also require security sensors and equipment, depending upon the level of protection and defensive layers needed. Reference: *U.S. Army TM 5-85*	
Security System Documents			
12.39	**Have security system as-built drawings been generated and are they ready for review?**	Drawings are critical to the consideration and operation of security technologies, including its overall design and engineering processes. These historical reference documents outline system specifications and layout security devices used, as well as their application, location, and connectivity. They are a critical resource tool for troubleshooting system problems, and replacing and adding other security system hardware and software products. Such documents are an integral component to new and retrofit construction projects. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.40	**Have security system design and drawing standards been developed?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.41	**Are security equipment selection criteria defined?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
12.42	**What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.43	**Have security system construction specification documents been prepared and standardized?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.44	**Do all security system documents include current as-built drawings?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.45	**Have qualifications been determined for security consultants, system designers/engineers, installation vendors, and contractors?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.46	**Are security systems decentralized, centralized, or integrated?** **Do they operate over an existing IT network or are they a standalone method of operation?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.47	**What security systems manuals are available?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
12.48	**What maintenance or service agreements exist for security systems?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
13	**Security Master Plan**		
13.1	**Does a written security plan exist for this site or building?** **When was the initial security plan written and last revised?** **Who is responsible for preparing and reviewing the security plan?**	The development and implementation of a security master plan provides a roadmap that outlines the strategic direction and vision, operational, managerial, and technological mission, goals, and objectives of the organization's security program. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
13.2	**Has the security plan been communicated and disseminated to key management personnel and departments?**	The security plan should be part of the building design so that the construction or renovation of the structure integrates with the security procedures to be used during daily operations. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.3	**Has the security plan been benchmarked or compared against related organizations and operational entities?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.4	**Has the security plan ever been tested and evaluated from a benefit/cost and operational efficiency and effectiveness perspective?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.5	**Does the security plan define mission, vision, and short- and long-term security program goals and objectives?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.6	**Are threats/hazards, vulnerabilities, and risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?**	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
13.7	**Has a security implementation schedule been established to address recommended security solutions?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
13	**Security Master Plan**		
13.8	**Have security operating and capital budgets been addressed, approved, and established to support the plan?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.9	**What regulatory or industry guidelines/standards were followed in the preparation of the security plan?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.10	**Does the security plan address existing security conditions from an administrative, operational, managerial, and technical security systems perspective?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.11	**Does the security plan address the protection of people, property, assets, and information?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.12	**Does the security plan address the following major components: access control, surveillance, response, building hardening, and protection against CBR and cyber-network attacks?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.13	**Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	
13.14	**When was the last security assessment performed?** **Who performed the security risk assessment?**	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	

Section	Vulnerability Question	Guidance	Observations
13	**Security Master Plan**		
13.15	**Are the following areas of security analysis addressed in the security master plan?** **Asset Analysis:** Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current value, and replacement value? **Threat Analysis:** Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? (possible criminal acts [documented and review of police/security incident reports] associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings) **Vulnerability Analysis:** Does the security plan address other areas associated with the site or building and its operations that can be taken advantage of to carry out a threat? (architectural design and construction of new and existing buildings, technological support systems [e.g., heating, air conditioning, power, lighting and security systems, etc.] and operational procedures, policies, and controls) **Risk Analysis**: Does the security plan address the findings from the asset, threat/hazard, and vulnerability analyses in order to develop, recommend, and consider implementation of appropriate security countermeasures?	This process is the input to the building design and what mitigation measures will be included in the facility project to reduce risk and increase safety of the building and people. Reference: *USA TM 5-853, Security Engineering*	

*Sources:
Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health (CDC/NIOSH) Publication No. 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, May 2002
Federal Emergency Management Agency (FEMA) FEMA 154, *Rapid Visual Screening of Buildings for Seismic Hazards: A Handbook*, 1988 (also, Applied Technology Council (ATC-21) by same name) FEMA 386-7, *Integrating Human-Caused Hazards Into Mitigation Planning*, September 2002 SLG 101, *Guide for All-Hazard Emergency Operations Planning,* Chapter 6, Attachment G, Terrorism, April 2001
General Services Administration (GSA) PBS – P100, *Facilities Standards for Public Buildings Service,* November 2002
Lawrence Berkeley National Laboratory (LBNL) LBNL PUB-51959, *Protecting Buildings from a Biological or Chemical Attack: Actions to Take Before or During a Release*, January 10, 2003
U.S. Air Force (USAF) *Installation Force Protection Guide*, 1997
U.S. Army (USA) Technical Manuals (TM) 5-853-1/-2/-3/-4, *Security Engineering*, May 12, 1994
U.S. Department of Commerce, Critical Infrastructure Assurance Office (DOC CIAO) *Vulnerability Assessment Framework 1.1*, October 1998
U.S. Department of Defense (DoD) Unified Facilities Criteria (UFC), UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, July 31, 2002
U.S. Department of Justice (DOJ) National Criminal Justice (NCJ) NCJ181200, *Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit*, May 15, 2000
U.S. Department of Veterans Affairs (VA) Physical Security Assessment for the Department of Veterans Affairs Facilities, *Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs*, 6 September 2002

ASSESSOR'S USER GUIDE*

Introduction **B1-3**

Before the Assessment: Getting Ready to Use the Assessors' Version of the Risk Assessmen-Database **B1-4**

Main Menu **B1-5**

Assessment Team B1-6

Points of Contact B1-7

GIS Portfolio B1-8

Miscellaneous Files B1-9

Critical Functions Matrix **B1-10**

Critical Functions Rollup B1-11

Critical Infrastructure Matrix **B1-12**

Critical Infrastructure Rollup B1-13

Observations and Recommendations/Remediations for the Vulnerability Assessment Checklist Sections **B1-14**

Select File **B1-15**

Importing Data from Other Databases **B1-16**

Importing Observation and Recommendation/Remediation Data B1-16

Observation Details from the REMOTE Database *B1-17*

Importing Vulnerability and Recommendation/Remediation Data B1-18

Assessment Vulnerabilities from the REMOTE Database *B1-19*

Assessment Main Page **B1-20**

Executive Summary B1-20

Vulnerabilities B1-21

Remediations *B1-22*

After the Assessment: Giving Data to the Database Administrator **B1-23**

*© National Institute of Building Sciences 2004

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

INTRODUCTION

To support the building assessment process, this easy to use Risk Assessment Database application is provided 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 collection tool and a 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, emergency plans, and certain Geographic Information System (GIS) products as part of the record of assessment. Managers can use the application to store, search, and analyze data collected from multiple assessments.

The Risk Assessment Database is initially installed on a desktop computer at an organization's headquarters. This database, referred to in this User Guide as the Manager's Database, becomes the main access and storage point for future assessment data. When an organization wants to conduct an assessment of a site or series of sites, a database administrator uses the application to produce a small temporary database, called the Assessor's Database, on a CD. Into this Assessor's Database are placed references, site plans, GIS portfolios, and other site-specific data that are known about the assessment site or are developed during the pre-assessment phase. This Assessor's Database is given to the Assessment Team and is loaded on one or more of their assessment computers (usually laptop computers). The Assessment Team then conducts their assessment and records information in the Assessor's Database. At the end of the assessment, the Assessment Team combines their data into one database and passes the files back to the database administrator. The administrator then loads the data into the Manager's Database for printing and analysis.

After initially installing the application, access to that Risk Assessment Database becomes restricted to only those designated users who have been assigned permission to access to the database by their administrator. Also, data can be viewed by all authorized users of the database, but changes to the data can only be made by those granted permission. All access permission questions should be directed to the database administrator of your organization.

The following are the hardware and software requirements for the Risk Assessment Database:

Pentium® 4 or equivalent processor
Windows XP
MS Access® 2002
256 MB of RAM recommended for all components

BEFORE THE ASSESSMENT: GETTING READY TO USE THE ASSESSOR'S VERSION OF THE RISK ASSESSMENT DATABASE

From your database administrator, the user should receive a folder named FEMA_452dB_Assessor containing the database application (3 files), assessment site(s) folder(s), which contain the folders,

and an application shortcut with the icon or .

- The **FEMA_452dB_Assessor folder** must be copied to the **C:\ drive**; the database application is dependent on the folder being downloaded to this location on the computer.

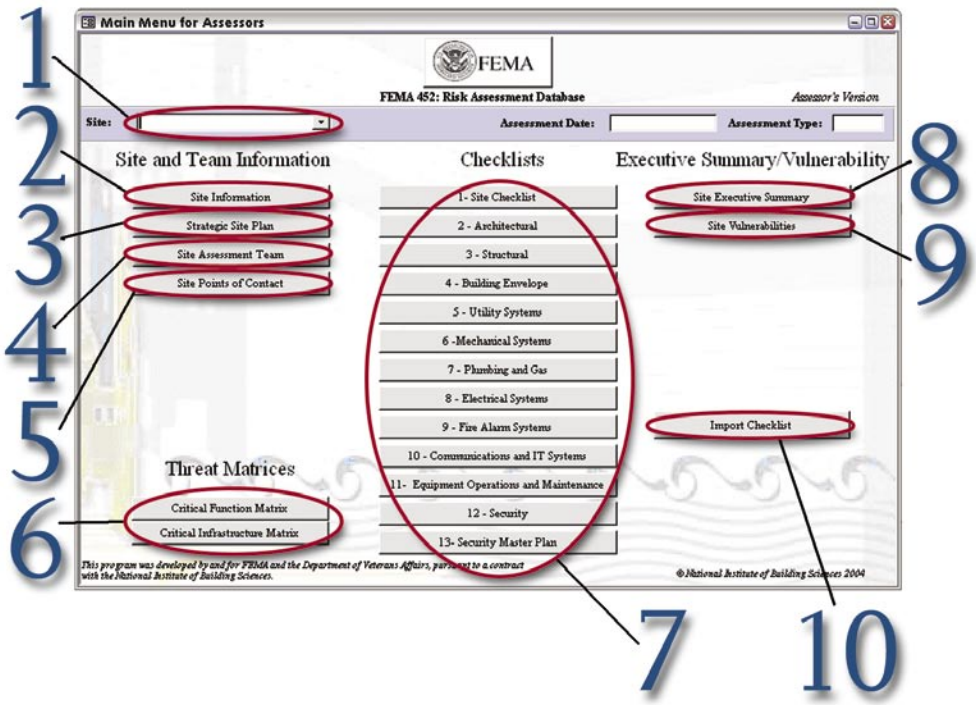
- The **application shortcut** should be copied to the **desktop**.

- When the user double clicks the application shortcut, the user receives a logon prompt:

- The user should log on using the user name and password provided by the database administrator.

- After logging in, the user will get the **Main Menu for Assessors**.

MAIN MENU



1. This is a drop down list of assessment sites. **An assessment site must be selected before any of the other buttons can be used.**

2. The ***Site Information*** button opens the **Site Information** report. This is not filled out by the on-site Assessor; it is usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

3. The ***Strategic Site Plan*** button opens the **Strategic Site Plan** in Microsoft Excel, if it is available. This is not filled out by the on-site Assessor; it is usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

4. The ***Site Assessment Team*** button opens the **Assessment Main Page** to the tab with information for the team that performed the assessment (**Assessment Team**).

5. The ***Site Points of Contact*** button opens the **Assessment Main Page** to the tab with the contact information for the assessment site points of contact (**Points of Contact**).

6. The ***Critical Function Matrix*** button opens the **Critical Functions Matrix**

form, and the ***Critical Infrastructures Matrix*** button opens the **Critical Infrastructures Matrix** form.

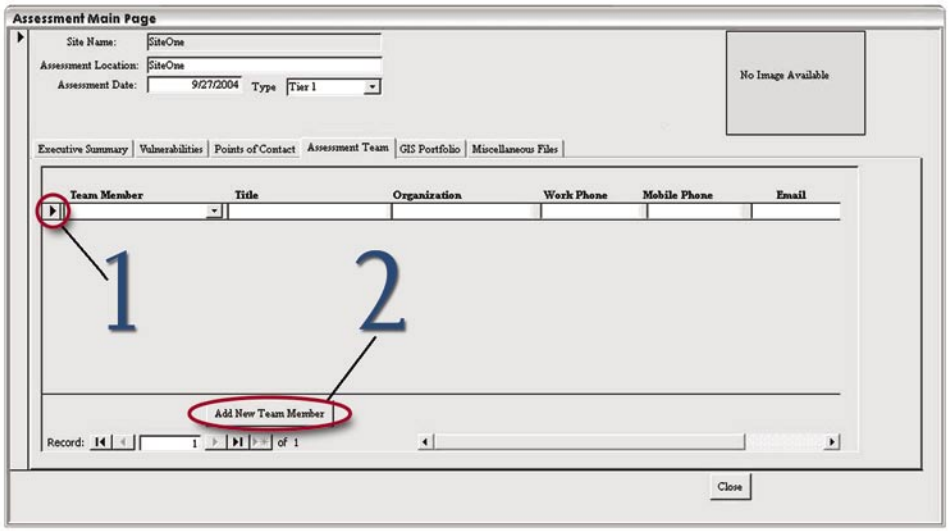
7. The ***Vulnerability Assessment Checklist*** buttons open a form that allows the user to input observations, recommendations/remediations, and vulnerability categorizations to the database for each checklist section. **(Observations and Recommendations/Remediations for Vulnerability Assessment Checklist Questions).**

8. The ***Site Executive Summary*** button opens the **Assessment Main Page** to the tab with the **Executive Summary**.

9. The ***Site Vulnerabilities*** button opens the **Assessment Main Page** to the tab with the **Vulnerabilities** for that assessment.

10. The Import Checklist button opens the **Select File** screen, which allows the main user to connect to another user's data for import.

Assessment Team

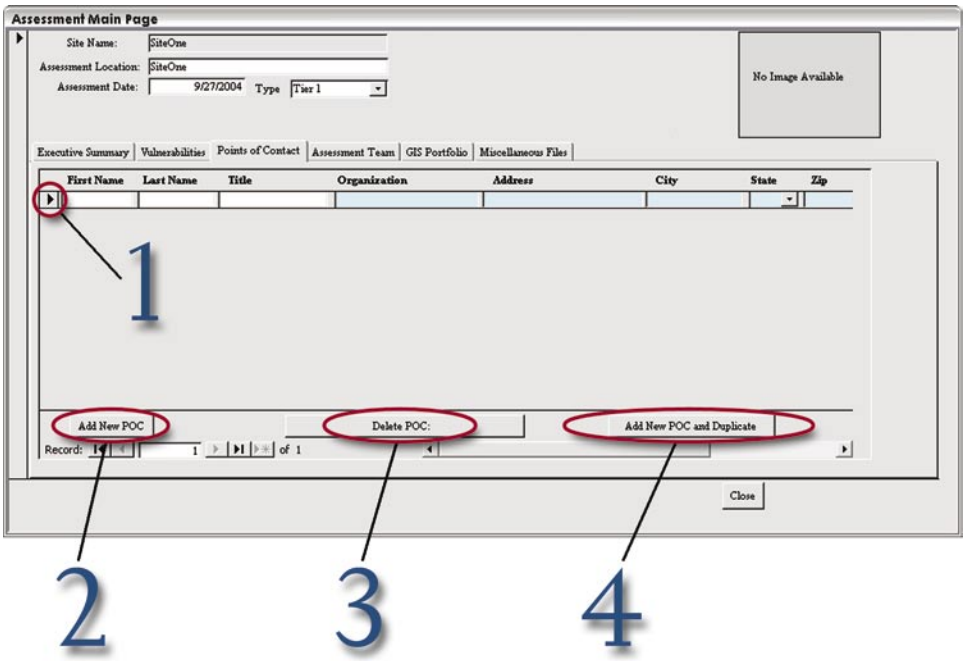


This form allows the user to enter information about Assessment Team members.

1. The black triangle indicates the record that is selected.

2. The ***Add New Team Member*** button allows for the creation of a new Assessment Team member for the assessment site designated in the upper left portion of this form.

Points of Contact



This form allows the user to enter information about points of contact (POC) at the assessment site.

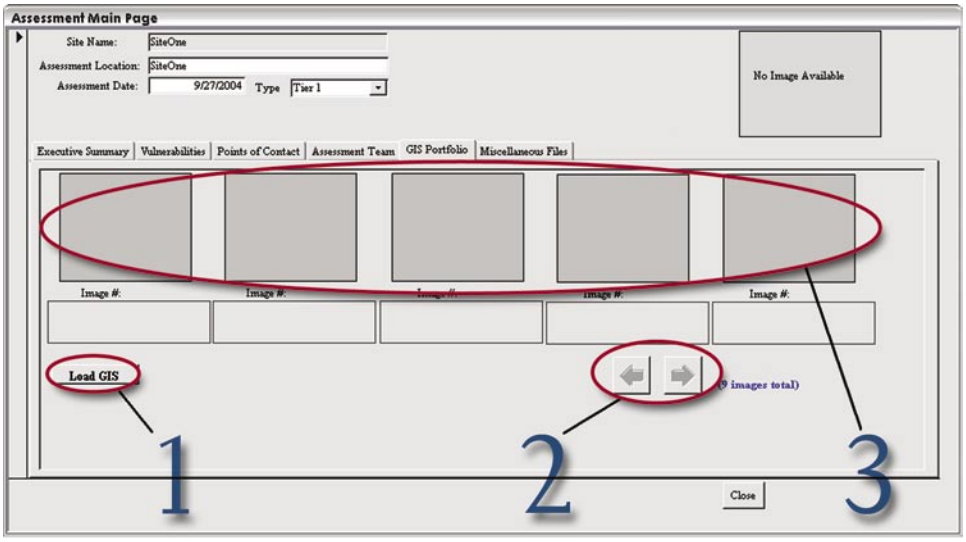
1. The black triangle indicates the record that is selected.

2. The ***Add New POC*** button allows for the creation of a new contact for the assessment site designated in the upper left portion of this form.

3. The **Delete POC** button allows the removal of the selected contact from the database.

4. The A***dd New POC and Duplicate*** button allows the creation of a new contact and duplicates the information in light blue in order to minimize data entry efforts.

GIS Portfolio



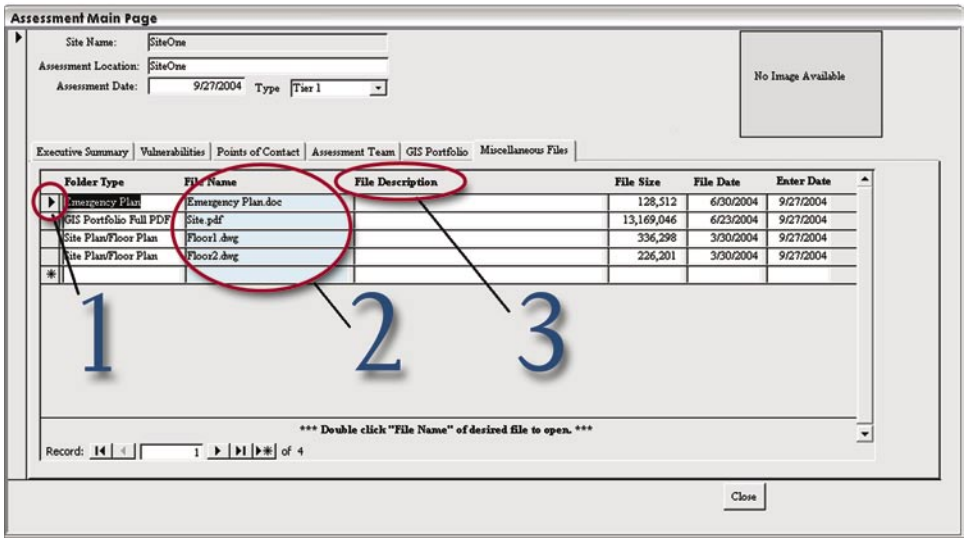
This form enables the user to see GIS images associated with the assessment site if developed during the pre-assessment period. These images are not entered by the on-site Assessor; the form is usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

1. The ***Load GIS*** button loads GIS images to the designated frames.

2. The 2 arrow button allows for navigation through pages of 5 GIS images, either to the previous 5 images or to the next 5 images.

3. Clicking on any of the GIS images will open the image in the ***Photo Zoom*** window, which displays the image larger, and the image can be printed individually in this window.

Miscellaneous Files



This form enables the user to see if files related to the assessment are available to view. (If developed during the pre-assessment period.) These images are not entered by the on-site Assessor; they are usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

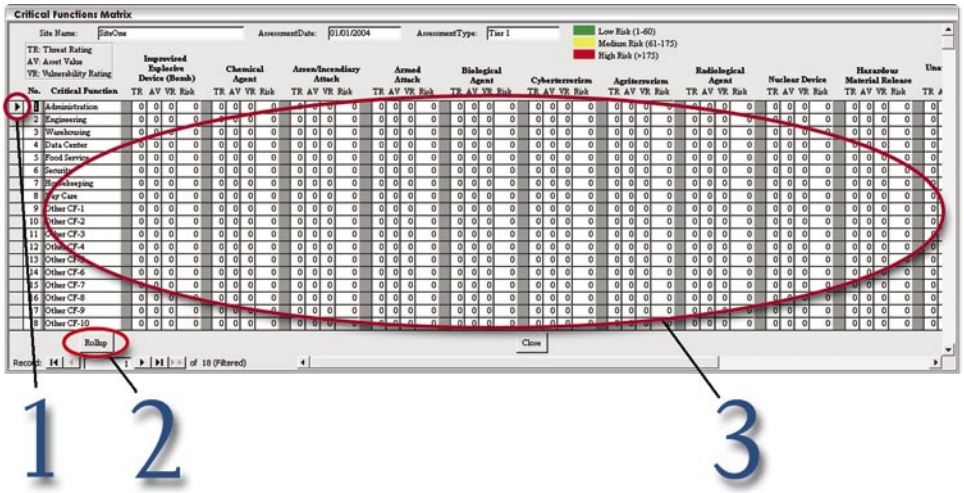
The form displays a list of the files available and allows the user to open and view the files.

1. The black triangle indicates the record that is selected.

2. Double-clicking any of the file names will open the associated file (examples of possible files to pre-load for the assessors include references, a GIS portfolio in PDF format, and/or past assessment reports).

3. The ***File Description*** field allows for descriptions to be typed in about each of the file names in the record.

CRITICAL FUNCTIONS MATRIX



This form records and numerically displays the results of analysis performed during the assessment. The matrix lists Critical Functions down the left side and threats across the top to create Threat-pairs. For each Threat-pair, a numeric value, on a 1-10 scale, is recorded for a threat rating, an asset value rating, and a vulnerability rating. The methodology for determining the ratings is found in FEMA 452.

1. The black triangle indicates the record that is selected.

2. The ***Rollup*** button opens a window that summarizes all of the risk columns into one easy to read form called **Critical Functions Rollup.**

3. These fields are where values (1-10) are typed in for each of the Threat-pairs. The Risk Column is automatically generated and color coded.

Critical Functions Rollup

Critical Infrastructure Rollup

Site Name: SiteOne

Assessment Date: 01/01/2004

Assessment Type: Tier 1

Low Risk (1-60)
Medium Risk (61-175)
High Risk (>175)

No.	Critical Infrastructure	IED (Bomb) Risk	Chem Agent Risk	Arson/ Incend. Risk	Armed Attack Risk	Bio Agent Risk	Cyber-terrorism Risk	Agri-terrorism Risk	Radio-logical Risk	Nuclear Device Risk	Hazmat Release Risk	Unauth. Entry Risk	Surveil-lance Risk	Suicide Bomber Risk	Other CI-1 Risk	Other CI-2 Risk
1	Site	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Architectural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Structural Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Envelope Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Utility Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Mechanical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Plumbing and Gas Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Electrical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Fire Alarm Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	IT/Communications Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Other CI-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Other CI-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Other CI-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Other CI-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Other CI-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Other CI-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Other CI-7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Other CI-8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	Other CI-9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	Other CI-10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Close

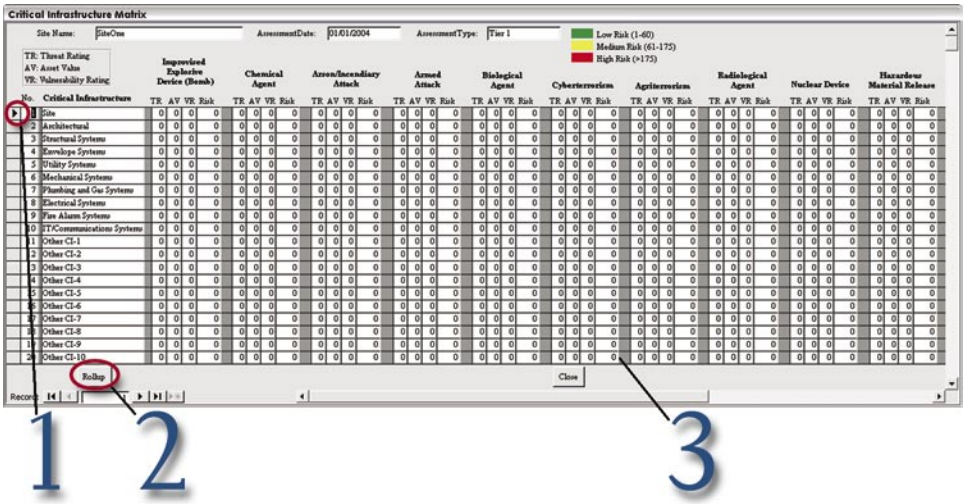
Record: 1 of 20 (Filtered)

1

This form displays a summary of the final numeric risk value of each Threat-pair in the **Critical Functions Matrix**.

1. The black triangle indicates the record that is selected.

CRITICAL INFRASTRUCTURE MATRIX



This form records and numerically displays the results of analysis performed during the assessment. The matrix lists Critical Infrastructure down the left side and threats across the top to create Threat-pairs. For each Threat-pair, a numeric value, on a 1-10 scale, is recorded for a threat rating, an asset value rating, and a vulnerability rating. The methodology for determining the ratings is found in FEMA 452.

1. The black triangle indicates the record that is selected.

2. The ***Rollup*** button opens a window that summarizes all of the risk columns into one easy to read called **Critical Infrastructure Rollup**.

3. These fields are where values (1-10) are typed in for each of the threats to a critical infrastructure.

Critical Infrastructure Rollup

Critical Infrastructure Rollup

Site Name: SiteOne

Assessment Date: 01/01/2004

Assessment Type: Tier 1

Low Risk (1-60)
Medium Risk (61-175)
High Risk (>175)

No.	Critical Infrastructure	IED (Bomb) Risk	Chem Agent Risk	Arson/ Incend. Risk	Armed Attack Risk	Bio Agent Risk	Cyber-terrorism Risk	Agri-terrorism Risk	Radio-logical Risk	Nuclear Device Risk	Hazmat Release Risk	Unauth. Entry Risk	Surveil-lance Risk	Suicide Bomber Risk	Other CI-1 Risk	Other CI-2 Risk
1	Site	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Architectural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Structural Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Envelope Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Utility Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Mechanical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Plumbing and Gas Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Electrical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Fire Alarm Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	IT/Communications Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Other CI-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Other CI-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Other CI-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Other CI-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Other CI-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Other CI-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Other CI-7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Other CI-8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	Other CI-9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	Other CI-10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Close

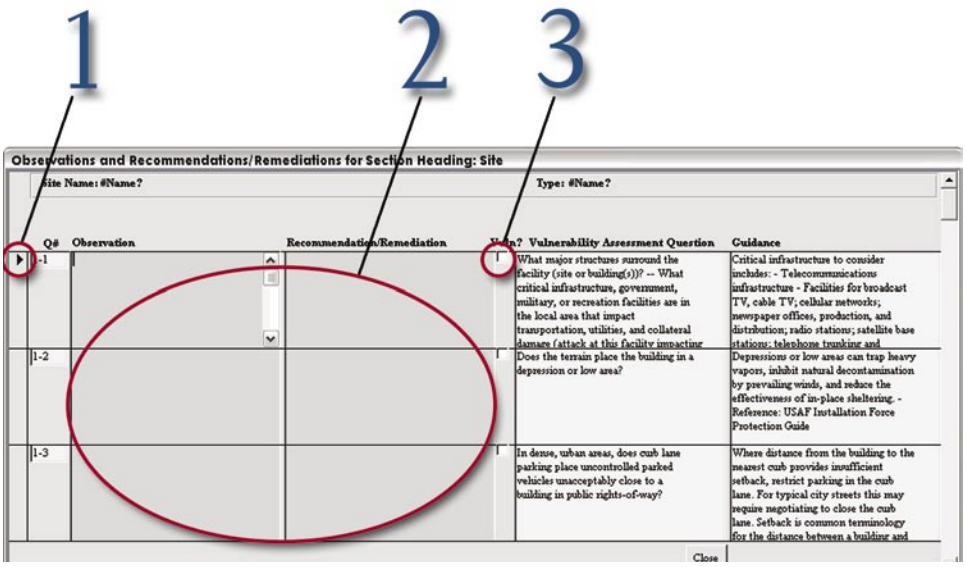
Record: 1 of 20 (Filtered)

1

This form is used to view the risk of threats for the specified critical infrastructure.

1. The black triangle indicates the record that is selected.

OBSERVATIONS AND RECOMMENDATIONS/ REMEDIATIONS FOR THE VULNERABILITY ASSESSMENT CHECKLIST SECTIONS



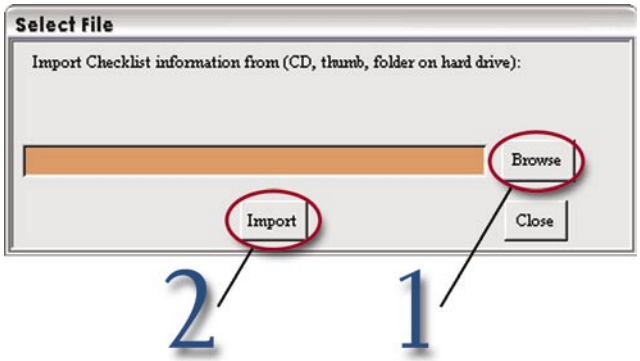
This form allows the user to enter observations and recommendations/remediations for each of the vulnerability assessment checklist questions.

1. The black triangle indicates the record that is selected.

2. These fields are where observations and recommendations/remediations are entered by the user.

3. This checkbox is selected if the observation is a vulnerability; the observations and recommendations/remediations are copied to the **Vulnerabilities** page.

SELECT FILE



If assessment data are collected and recorded on more than one computer, this form allows the "main user" to connect to another user's database, and import the other user's data. Note: the threat matrices cannot be imported, so it is important for the "main user" to have the threat matrices data in their database.

1. The ***Browse*** button allows the user to search for and select another database to connect to. (Note: The database to connect to will have "Data" in its name, not "Application.")

2. The ***Import*** button allows the user to connect the database selected in 1.

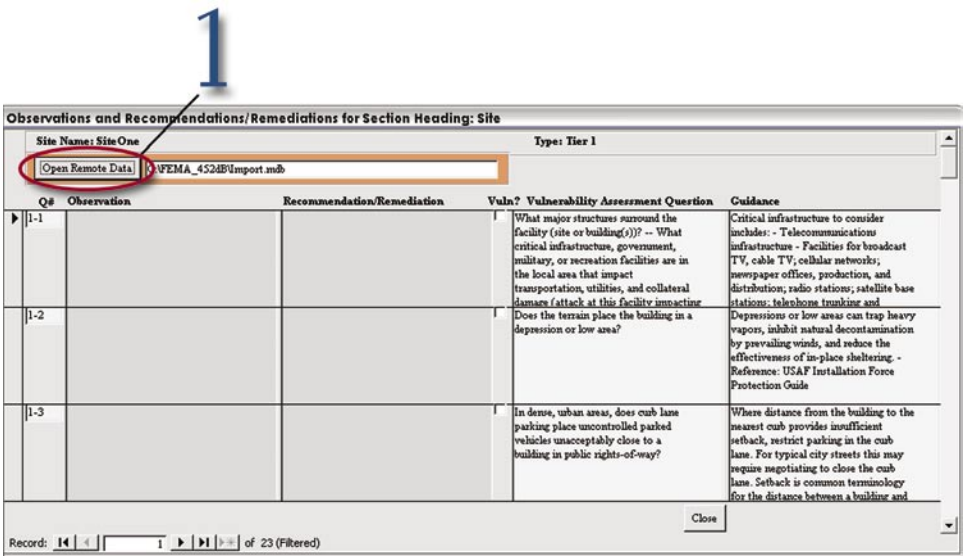
Once a connection is made, this window will pop up. Simply click the ***OK*** button to make the data available for viewing or copying.

IMPORTING DATA FROM OTHER DATABASES

After a database connection has been made (see **Select File**), the user can start importing another user's data.

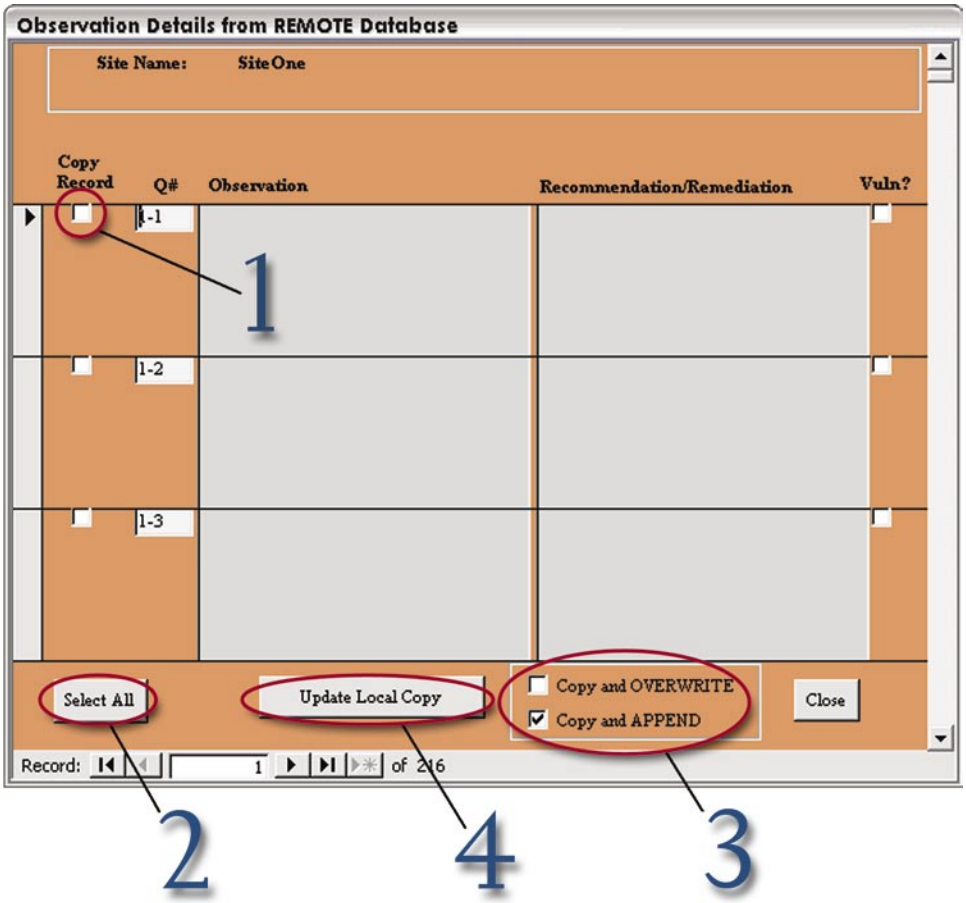
Importing Observation and Recommendation/ Remediation Data

Once connected to another database, the **Main Menu** screen will appear the same. Clicking on any of the Vulnerability Assessment Checklist buttons will supply this window with a new ***Open Remote Data*** button added to the screen.



1. The ***Open Remote Data*** button will make the additional data available and open the **Observation Details from REMOTE Database** screen.

Observation Details from the REMOTE Database



This form displays the remote data and allows the Main User to choose which data to import.

1. This checkbox allows the user to select individual records to be imported.

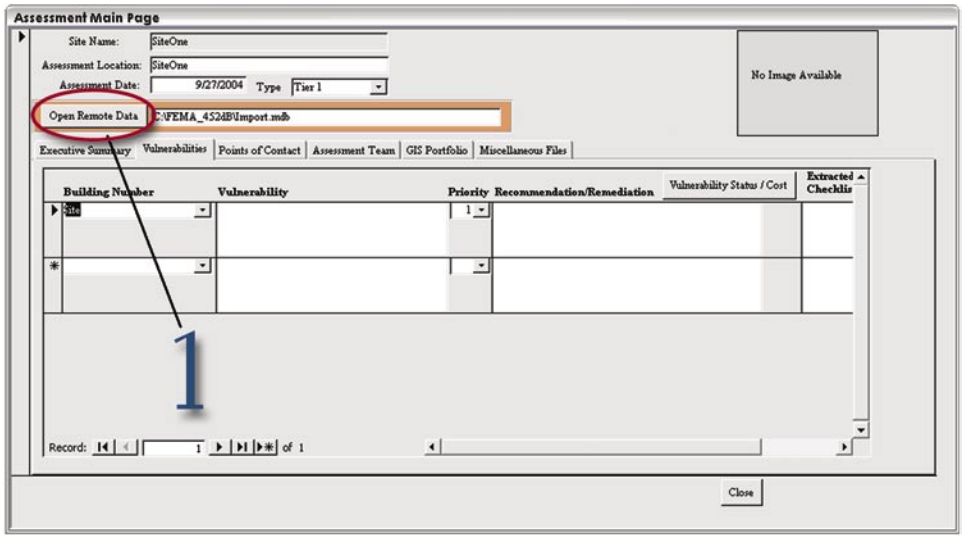
2. The ***Select All*** button selects all of the records.

3. These checkboxes are options for copying another user's data. The ***Copy and OVERWRITE*** checkbox will overwrite the data in the user's database; the ***Copy and APPEND*** checkbox will add the other user's data to the data existing in the user's database.

4. The ***Update Local Copy*** button is the final step and copies the data into the main user's database

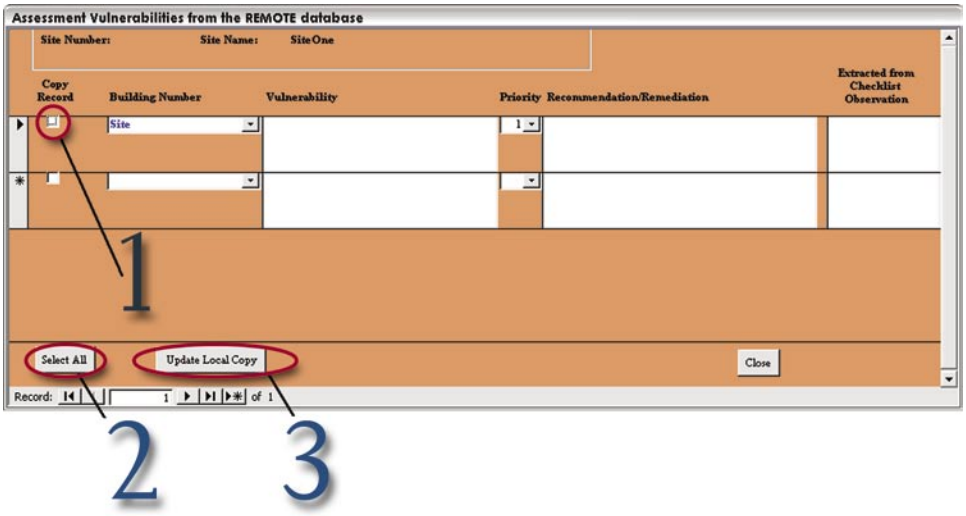
Importing Vulnerability and Recommendation/ Remediation Data

Once connected to another database, the **Main Menu** screen will appear the same. Clicking on the ***Site Vulnerabilities*** button will supply this window with a new ***Open Remote Data*** button added to the screen.



1. The ***Open Remote Data*** button will make the additional data available and open the **Observation Details from REMOTE Database** screen.

Assessment Vulnerabilities from the REMOTE Database



This form displays the remote data and allows the main user to choose which data to import.

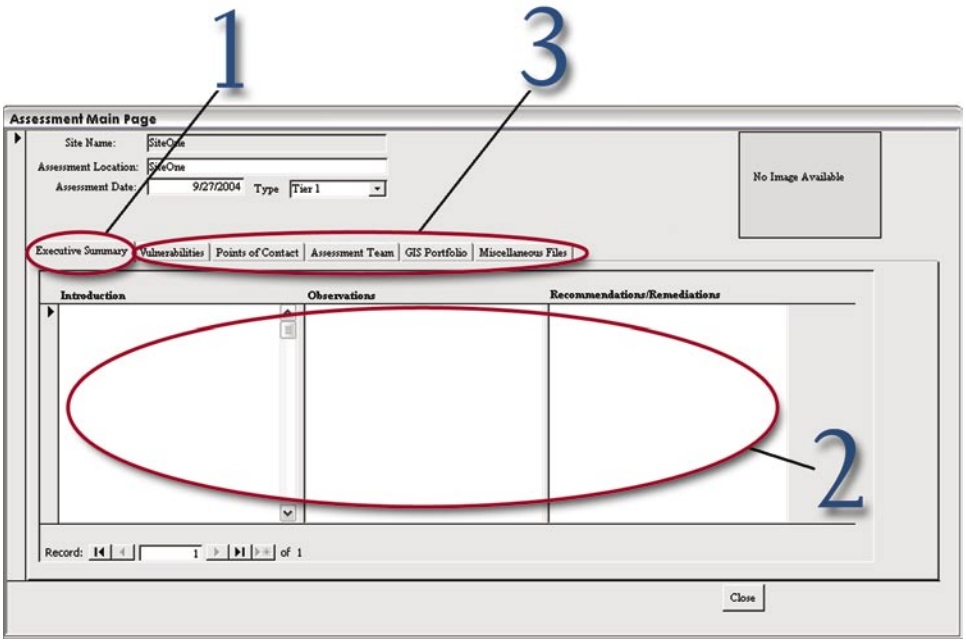
1. This checkbox allows the user to select individual records to be imported.

2. The ***Select All*** button selects all the records.

3. The ***Update Local Copy*** button is the final step and copies the data into the main user's database.

ASSESSMENT MAIN PAGE

Executive Summary



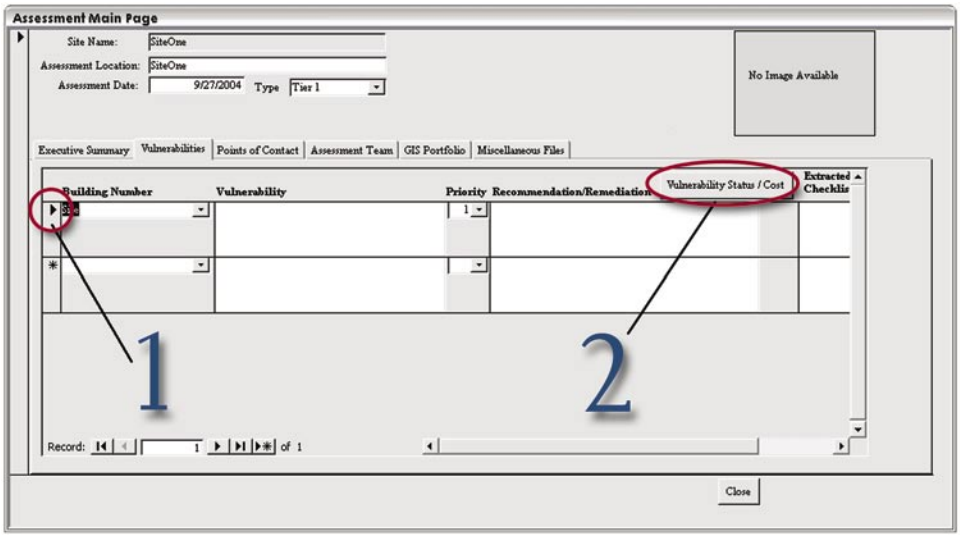
This form allows the user to enter an **Executive Summary** for the assessment site report.

1. The first tab is the **Executive Summary** input form for the site selected in the drop down list on the **Main Menu**.

2. This information is the first three paragraphs of the final assessment report and usually contains broad over arching information. Individual details are usually listed later in the vulnerability section of the report.

3. The page also allows users to navigate to other forms in the database without having to return to the main screen as follows:

Vulnerabilities

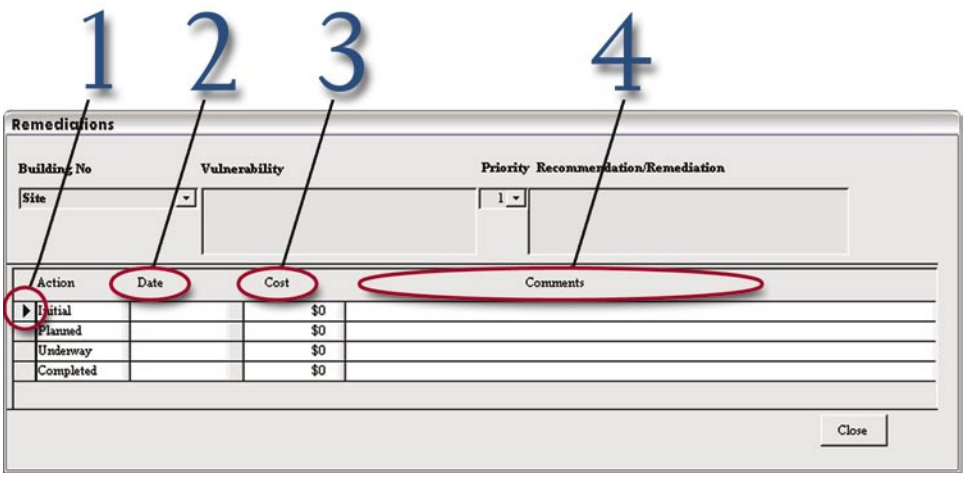


This form allows the user to enter additional information on the vulnerabilities and recommendations/remediations observed while performing the assessment. The form is linked to the **Observations and Recommendation/Remediation** form. Observations that were previously identified and "checked" as a vulnerability are automatically loaded into this form. These vulnerabilities should now be furthered analyzed and assigned a priority, a location, and a remediation cost estimate. (Note: Priority and Building Number are required.)

1. The black triangle indicates the record that is selected.

2. The ***Project Status/Cost*** button opens the **Remediations** form.

Remediations



This form allows the user to enter any remediation information related to an observed vulnerability, including date, cost, and comments.

1. The black triangle indicates the record that is selected.

2. This date field can be filled in by the user to keep the remediation cost records up to date.

3. Enter the cost for the remediation into this field to keep the remediation records up to date.

4. Enter any comments for the remediation in this field.

AFTER THE ASSESSMENT: GIVING DATA TO THE DATABASE ADMINISTRATOR

All of the assessment data should be in **one database**, the "main user's."

1. Once the database is complete, make sure all of the files are in the proper folder locations for each of the assessment site folders in the FEMA_452dB_Assessor folder. (Photos in the Photos folder, digital floor plans (such as CADD) in the Site_and_Floorplans folder, and emergency management plans in the Emergency_Plans folder.)

2. Provide the database administrator with a database file containing the word "Data," the Photos folder, the Site_and_Floorplans folder, and the Emergency_Plans folder.

DATABASE ADMINISTRATOR'S USER GUIDE*

Microsoft Access Experience **B2-3**

Before Using the Database **B2-3**

Database Specifics B2-3

Files to be Integrated into the Database – Assessment Supporting Materials B2-4

Beginning to Use the Database **B2-5**

Security B2-6

Administrative Functions **B2-7**

Load 'Miscellaneous' Files B2-8

Assessment Locations B2-9

Loading Photos and GIS Images **B2-10**

Assessor's Database **B2-12**

Creating an Assessor Database B2-12

Preparation: Assessment Supporting Information *B2-12*

Working in the Front End *B2-13*

Working in the Back End *B2-14*

Providing an Assessor with the Database Application B2-15

Importing the Assessor Data into the Main Database B2-15

Linked Table Manager **B2-16**

*© National Institute Of Building Sciences 2004

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

MICROSOFT ACCESS EXPERIENCE

It is highly recommended that the database administrator is an intermediate to advanced Microsoft Access user.

For up to date information about Microsoft Access, the software webpage is: http://office.microsoft.com/en-us/FX010857911033.aspx.

BEFORE USING THE DATABASE

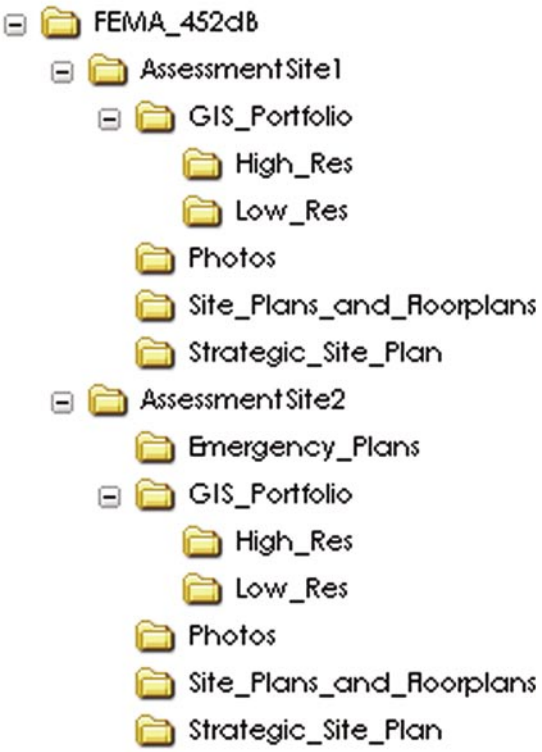
Database Specifics

The database application is composed of various files, including a Microsoft Access front end database ***(FEMA452_Application_v1.mde)***, a back end database ***(FEMA452_Data.mde)***, a workgroup file ***(FEMA452wg.mdw)***, a shortcut to the database ***(FEMA 452 Database)***, a shortcut to the back end of the database (**Master Data**), a Microsoft Word Document ***(FEMA452dB_UserGuide.doc)***, and a Microsoft Excel Spreadsheet ***(ThreatMatrix.xls)*** for the Master Database. An assessor database front end and front end shortcut are provided ***(FEMA452db_App_Assessor_v1.mde and FEMA 452 Assessor Database,*** respectively). Also, a short cut to the workgroup file ***(Workgroup)***, to change passwords and add users is provided.

The following are the hardware and software requirements for the Risk Assessment Database:

Pentium® 4 or equivalent processor
Windows XP
MS Access® 2002
256 MB of RAM recommended for all components

The database application files are set to run on the **C: drive**, in the **FEMA_452dB folder.** Similarly, the assessor database is set to run on the **C: drive**, in the **FEMA_45dB_Assessor folder.** The database applications have a specific file structure that has to be adhered to for the database to function properly, regardless of location on the computer.



Note: AssessmentSite1 and AssessmentSite2 are just example folders, and these will be replaced by assessment site folders created by the database administrator.

Files to be Integrated into the Database – Assessment Supporting Materials

Assessment support materials that can be integrated into this database include:

- Emergency plans,
- GIS materials – an Adobe PDF format portfolio, high and low resolution images (both high and low resolution images MUST have the same name, but with the low resolution image ending in "_lr"),

- Photos,
- Site plans and floor plans (CAD, Image), and
- Strategic site plan (Microsoft Excel spreadsheet).

All of these materials MUST be placed in the correct folders for the database application to be able to utilize them properly. See the following table for supporting material placement:

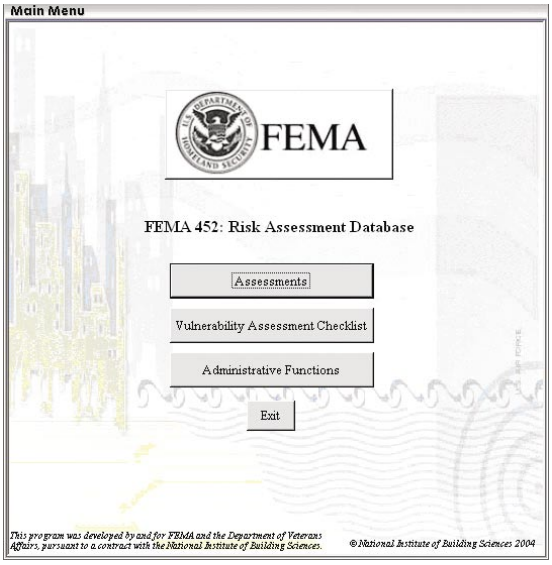
Supporting Material	Folder
Emergency plans - any format	Emergency_Plans
GIS materials - PDF	GIS_Portfolio
GIS materials - high resolution jpegs	High_Res
GIS materials - low resolution jpegs	Low_Res
Photos - jpegs	Photos
Site plans and floor plans (CAD, Image) - any format	Site_Plans_and_Floorplans
Strategic site plan - Microsoft Excel spreadsheet	Strategic_Site_Plan

All of these folders need to be utilized in the created Assessment Site folder, which is named while creating a new assessment location.

BEGINNING TO USE THE DATABASE

During Installation, a shortcut was placed on the desktop, "FEMA 452 Database." Double click the shortcut, and log on with the username "Administrator," with password administrator.

The **Main Menu** will open:



Security

Three user groups have been created, **Admins, Full Data Users,** and **Read Only Users**. Be sure to assign "Administrator" a different password after initial logon.

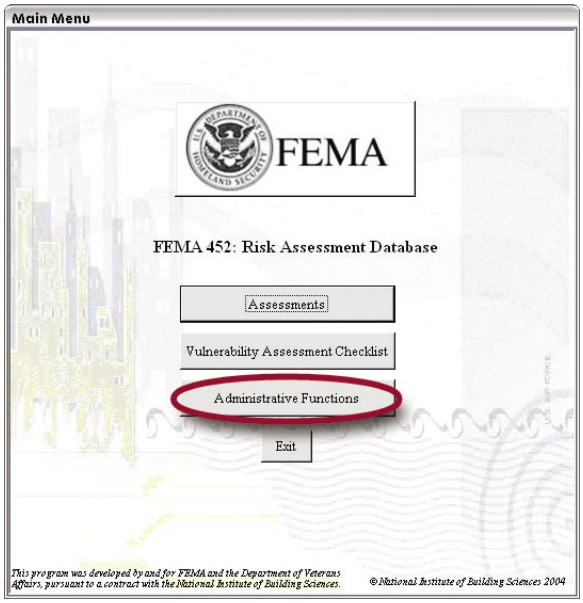
Admins has full access to the database. The ***Administrative Functions*** button will only be visible for users in the Administrator group. Two users have been created in this group, **Administrator** and **Assessor**. Both have initial passwords of "Administrator" and "Assessor," respectively.

Full Data Users can view and update data. The created user "Editor" has an initial password of "Editor."

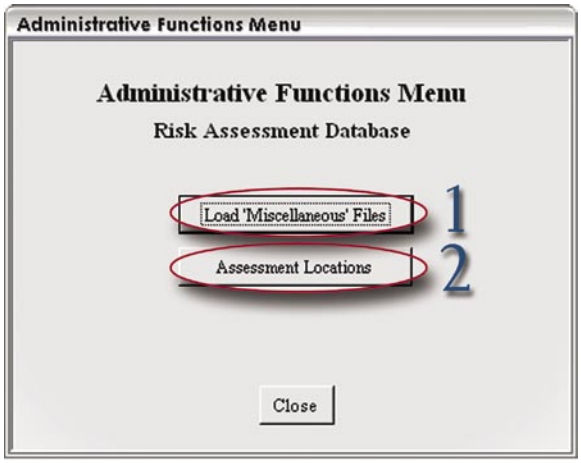
Reader can only view data. The created user "Reader" has an initial password of "Reader."

Add users as necessary using the Workgroup short cut provided.

ADMINISTRATIVE FUNCTIONS

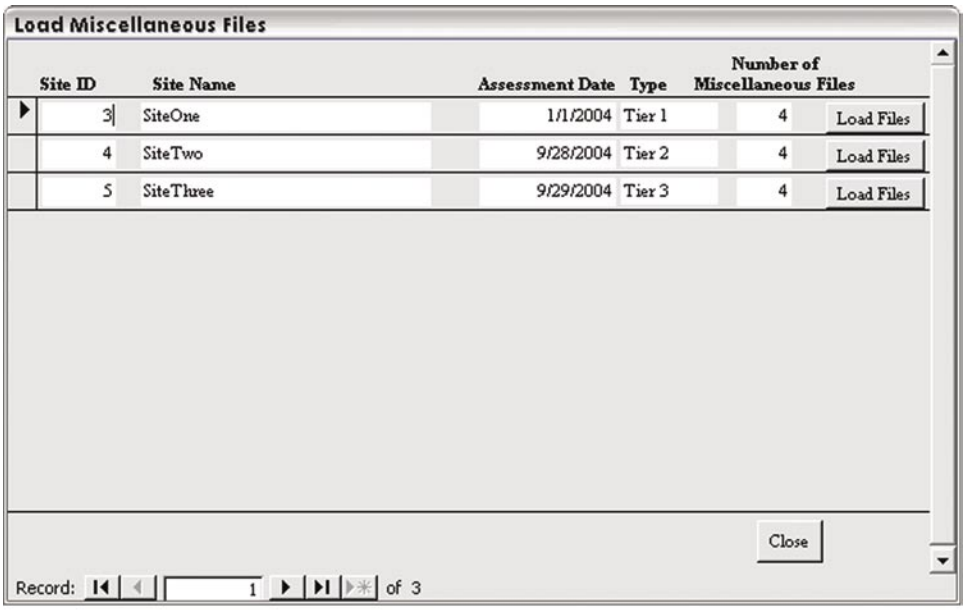


From the **Main Menu**, click the ***Administrative Functions*** button, and the **Administrative Functions Menu** will open:



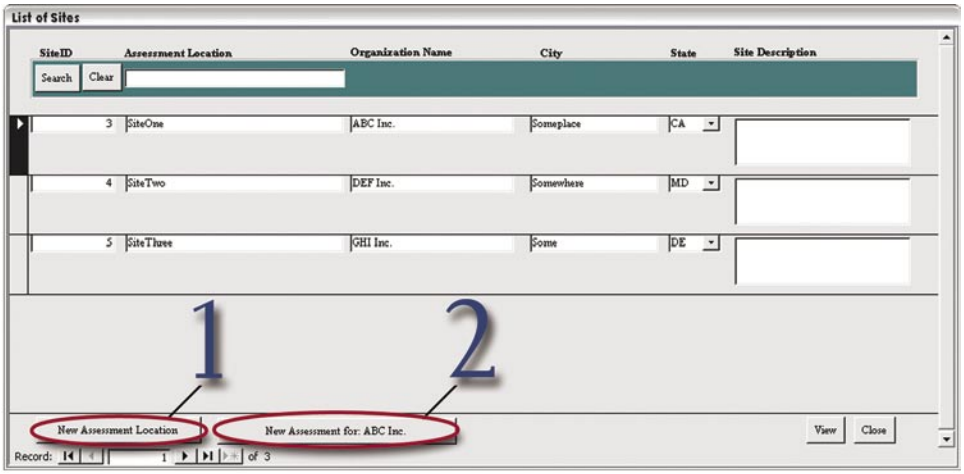
Load 'Miscellaneous' Files

This form allows the administrator to load files, including the **GIS Portfolio PDF, emergency plans**, and **site plans/floor plans,** so database users can access these files. These files must be in the correct location. See **Assessment Supporting Materials**.



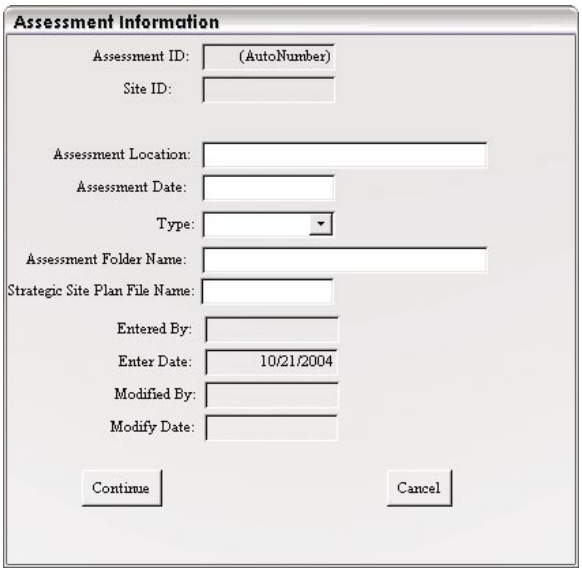
Assessment Locations

This form is where the database administrator can add new assessment locations and add questions and matrices to each of the assessment locations.



1. The ***New Assessment Location*** button opens a form for the input of a new assessment location.

2. The ***New Assessment for: (Organization Name)*** button opens a form **Assessment Information**:

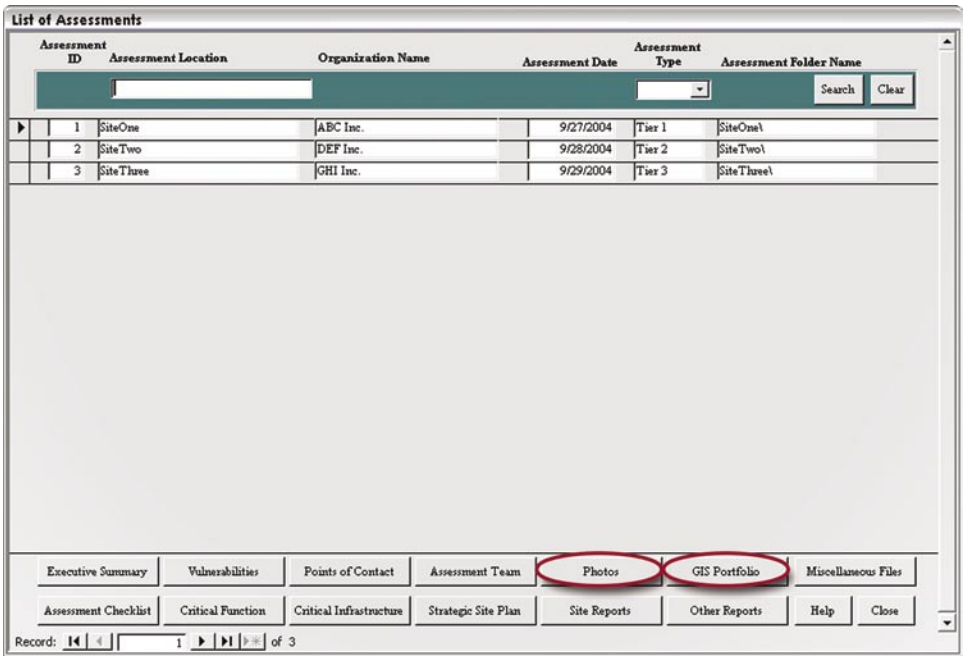


This form must be completed to create a new assessment. It is important to enter all of the information on this form correctly, as the database application uses the fields **Assessment Folder Name** and **Strategic Site Plan File Name** as "pointers," to access **Assessment Supporting Information**.

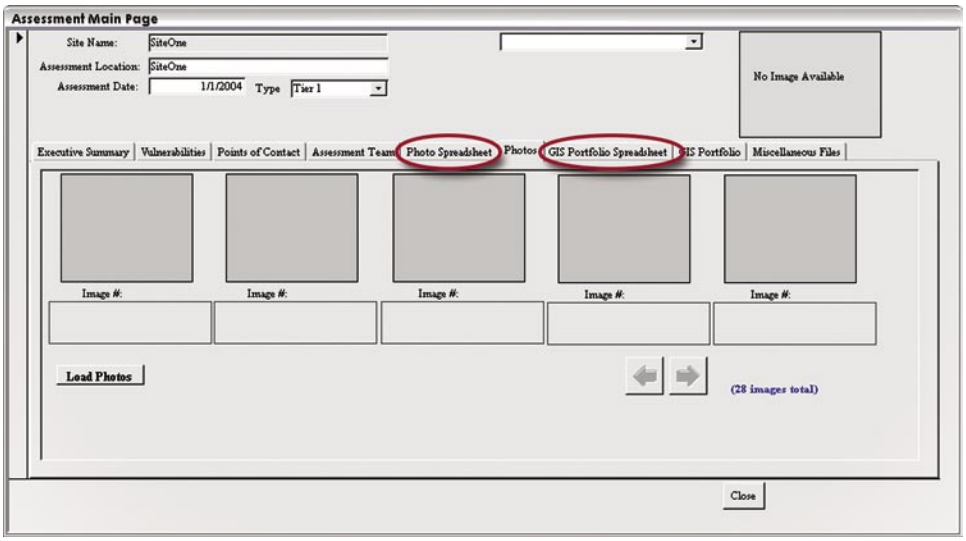
LOADING PHOTOS AND GIS IMAGES

The Administrator Group is the only group that has the permissions required to load photos and GIS images. To load the photos and GIS images into the database application:

1. Go to the **Main Menu**, and click on the ***Assessments*** button, which will open the **List of Assessments** page:



2. Click on either the ***Photos*** or the ***GIS Portfolio*** button (both circled in previous image), both of which will open the **Assessment Main Page**:



3. Click on the ***Photo Spreadsheet*** or the ***GIS Portfolio Spreadsheet*** button (both circled in previous image), both of which will open a new form:

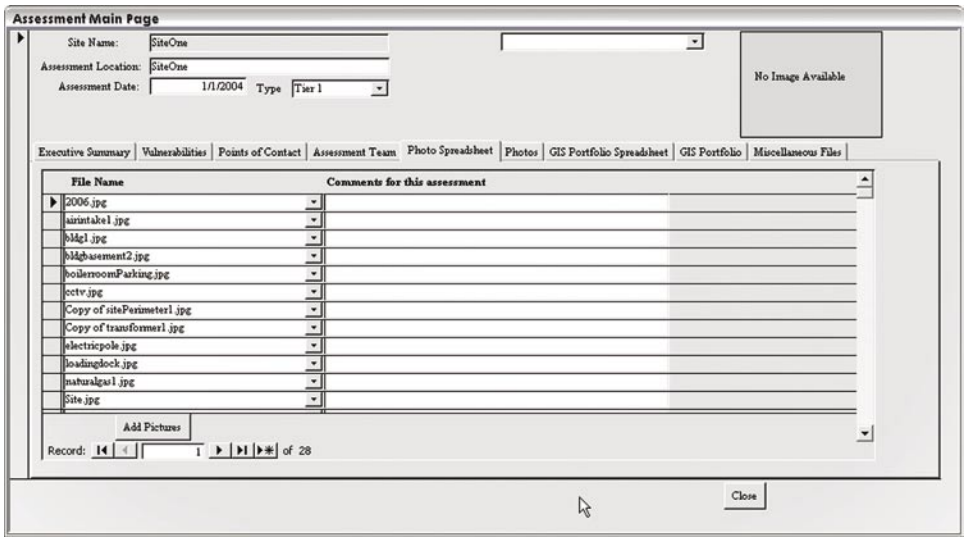
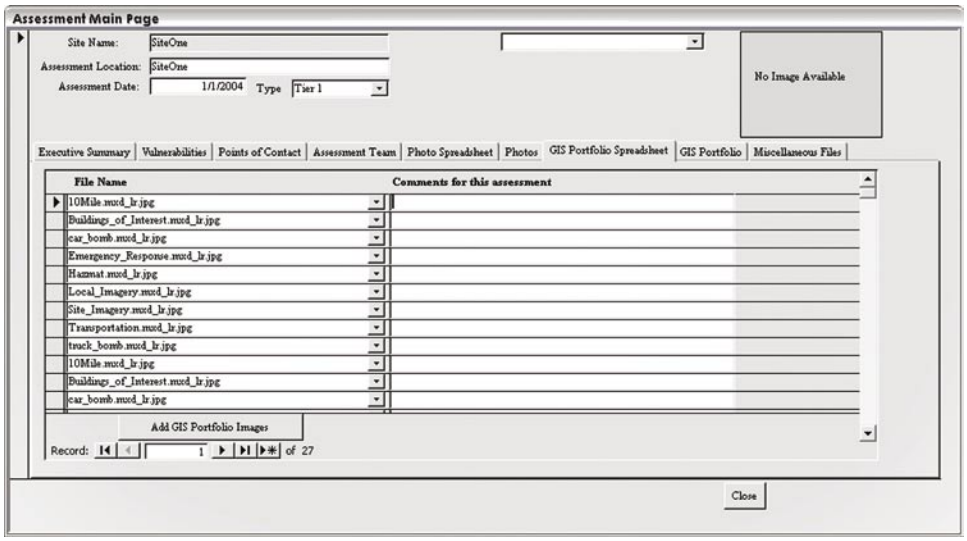


Photo Spreadsheet or the **GIS Portfolio Spreadsheet**



4. Add photos and/or GIS images by clicking either the ***Add Photos*** button or the ***Add GIS Images*** button.

ASSESSOR'S DATABASE

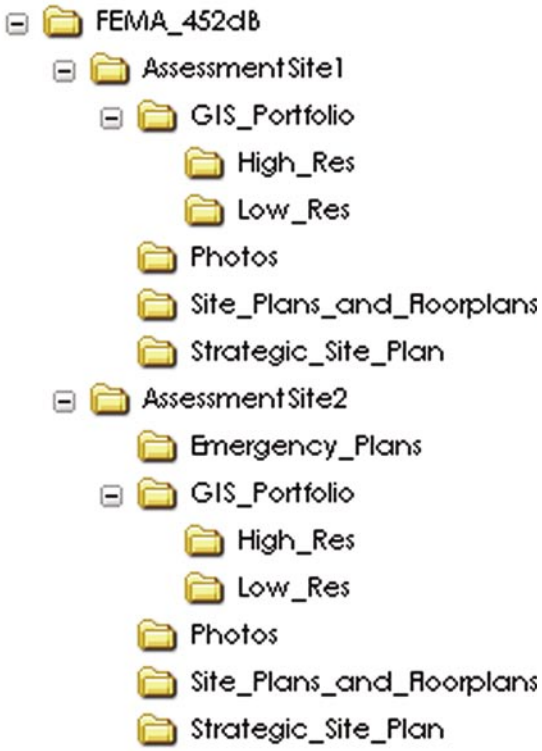
The CD includes a folder containing the assessor front end database ***(FEMA_452db_App_Assessor_v1.mde)***. To make this application function, the administrator will have to provide the assessor with a back end database, **FEMA452dB_Data.mde** and **Assessment Supporting Information**.

Creating an Assessor Database

An assessor database can be created following these steps:

Preparation: Assessment Supporting Information

1. Create an assessment site folder (it can be named anything as long as it is referenced properly when completing Assessment Information in step 4), and populate all of the **Assessment Supporting Information** folders with desired files. Be sure to keep the following file structure:



2. Copy and paste all of the assessment site folders to the C:\FEMA_452dB_Assessor folder.

Working in the Front End

1. Open the FEMA452dB_application_v1.mde, logging on as an Administrator.

2. Create a logon account for the assessor (if one is not created already).

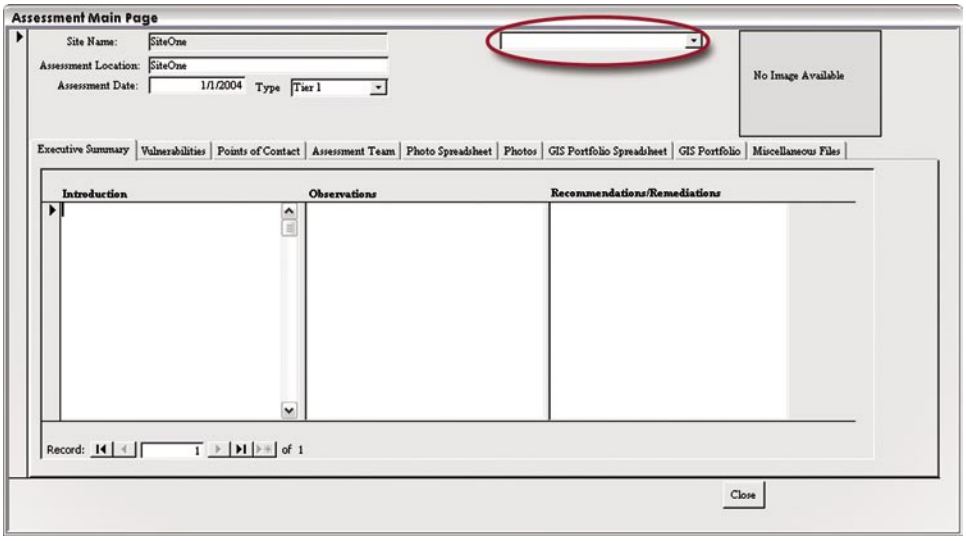
3. Create (an) assessment location(s) using the ***New Assessment Location*** function on the **Assessment Locations** form.

4. Create (a) new assessment(s) using the ***New Assessment for: (Organization just created)*** button function on the **Assessment Locations** form.

5. **Load any miscellaneous files** that may support the assessment.

6. **Load any photos or GIS images** that may have been taken or created for the assessment.

7. A default photo for the assessment, which will appear on the **Assessments Main Page** in the assessor's database, may be selected using the drop down menu located on the **Assessment Main Page**:



8. Close the database.

Working in the Back End

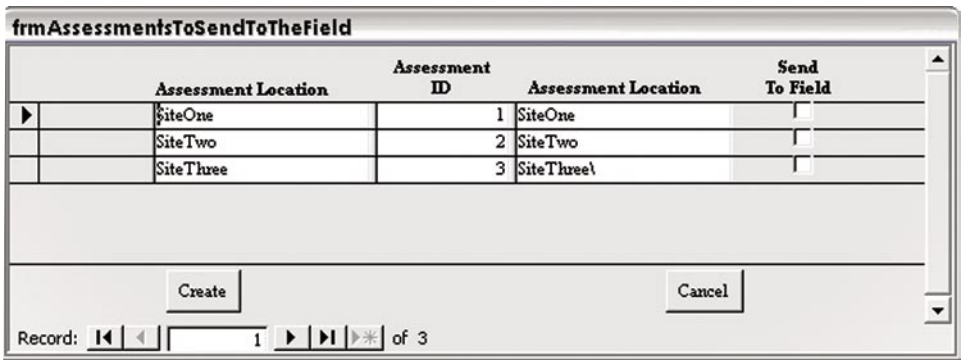
Only step 1 is necessary if this is the first assessment to go to the field, there is only one assessment, or if there is only one group of assessments

1. Copy the **FEMA452dB_Data.mde** and **FEMA452wg.mdw** file, and **paste it in the C:\FEMA_452dB_Assessor** folder.

The purpose of the following steps is to safeguard any sensitive material that may have been collected on previous assessments. After completing these steps, assessors will only be able to access information provided to them.

2. Open the FEMA452dB_Data.mde file by double clicking on the ***Assessor Data*** shortcut and logging on as the administrator, to open the **Administrative Functions Menu**:

3. Click the ***Create Field Database*** button to open the **Assessments to Send to the Field** form:



4. For any sites you want to send to the field, click the corresponding boxes for the site in the "Send To Field" column.

5. Click the ***Create*** button. (This is a destructive process – all of the assessment locations that are not marked will be completely deleted from the database.)

6. Compact and repair the database (Tools → Database Utilities → Compact and Repair Database…).

7. Close the database.

Providing an Assessor with the Database Application

The assessor needs the **FEMA_452dB_Assessor folder** in its entirety (database front-end, database back-end, workgroup file, assessment supporting materials) and the **FEMA 452 Assessor Database shortcut**. Be sure to **provide the assessor with their logon name and password (without any security changes**, this will be "Editor" and "Editor," respectively.

Burn this folder and files to a CD, put it on a USB drive, or post them on a ftp site to which the assessor has access.

Importing the Assessor Data into the Main Database

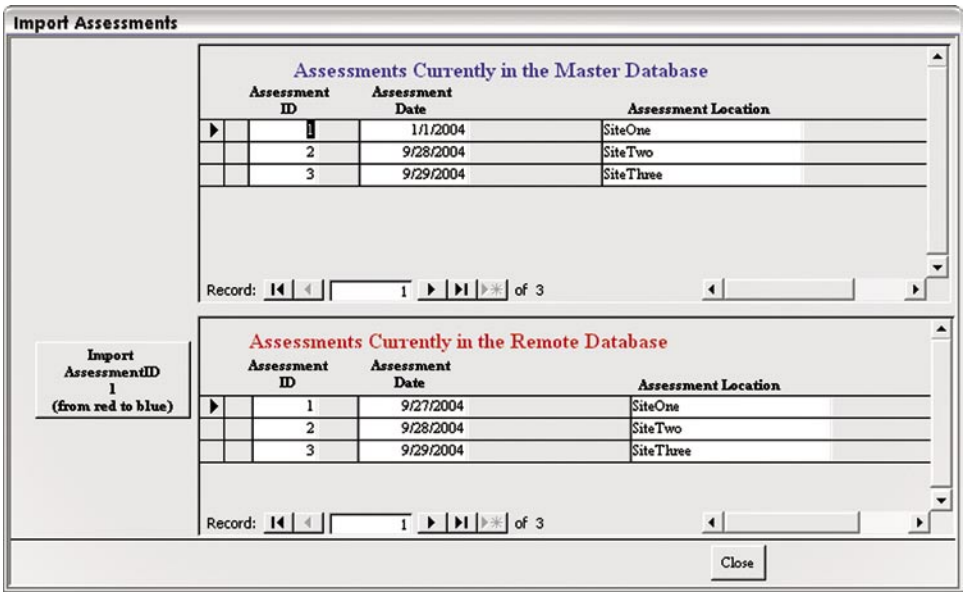
1. Open the **FEMA452dB_Data.mde** file using the ***Assessor Data*** shortcut and Administrator logon.

2. Link the following back-end tables to the **FEMA452_Data.mde** database the assessor provided using the **Linked Table Manager**.

    - tblAssessmentPeople1,
    - tblAssessmentVulnerabilities1,
    - tblBuildings1,
    - tblCFMatrix1,
    - tblCIMatrix1,
    - tblExecutiveSummary1,
    - tblObservations1, and
    - tblPeople1.

3. Compact and repair database (Tools → Database Utilities→ Compact and Repair Database…).

4. From the **Administrative Main Menu**, click the ***Import Data From Field*** button to get the **Import Assessments** form:



5. Make sure the record you want to import from the assessor's database is selected in both the Master Database and the Remote Database.

6. Click the ***Import Assessment ID (#)*** (from red to blue) button and click **OK** for all options for all assessment location data you want to import.

7. Compact and repair database (Tools → Database Utilities → Compact and Repair Database…).

8. Close the database.

LINKED TABLE MANAGER

The Linked Table Manager is utilized to link the back end database to an assessor database when importing data from the field.

The Linked Table Manager is accessed on the toolbar:

MANAGER'S USER GUIDE*

Introduction **B3-3**

Before Using the Database: Access to the Manager's Version of the Risk Assessment Database **B3-4**

Main Menu **B3-5**

List of Assessments **B3-6**

Assessment Main Page **B3-8**

Executive Summary B3-8

Vulnerabilities B3-9

Remediations *B3-10*

Points of Contact B3-11

Assessment Team B3-12

Photos B3-13

Gis Portfolio B3-14

Miscellaneous Files B3-15

Assessment Checklists **B3-16**

Critical Functions Matrix **B3-17**

Critical Functions Rollup B3-18

Critical Infrastructure Matrix **B3-19**

Critical Infrastructure Rollup B3-20

Site Assessments Reports Menu **B3-21**

Keyword Search Reports Menu **B3-22**

Observations and Recommendations/Remediations for Assessment Checklist B3-23

Vulnerabilities and Recommendations/Remediations B3-24

Assessment Checklist Question Details **B3-25**

All Observations and Recommendations/Remediations for This Question B3-26

Printing Reports and Accompanying Materials B3-27

Printing Assessment Sections Completed by Assessors..... B3-27

Printing Photos, GIS Portfolio, Floor Plans, Emergency Plans, and Other Related Documents B3-29

Printing Photos B3-29

Printing GIS Portfolio, Floor Plans, Emergency Plans, and Related Documents B3-31

*© National Institute Of Building Sciences 2004

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

INTRODUCTION

To support the building assessment process, this easy to use Risk Assessment Database application is provided 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 collection tool and a 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, emergency plans, and certain Geographic Information System (GIS) products as part of the record of assessment. Managers can use the application to store, search, and analyze data collected from multiple assessments.

The Risk Assessment Database is initially installed on a desktop computer at an organization's headquarters. This database, referred to in this User Guide as the Manager Database, becomes the main access and storage point for future assessment data. When an organization wants to conduct an assessment of a site or series of sites, a database administrator uses the application to produce a small temporary database, called the Assessor's Database, on a CD. Into this Assessor's Database are placed references, site plans, GIS portfolios, and other site-specific data that are known about the assessment site or are developed during the pre-assessment phase. This Assessor's Database is given to the assessment team and is loaded on one or more of their assessment computers (usually laptop computers). The Assessment Team then conducts their assessment and records information in the Assessor's Database. At the end of the assessment, the Assessment Team combines their data into one database and passes the files back to the database administrator. The administrator then loads the data into the Manager's Database for printing and analysis.

After initially installing the application, access to that Risk Assessment Database becomes restricted to only those designated users who have been assigned permission to access to the database by their administrator. Also, data can be viewed by all authorized users of the database, but changes to the data can only be made by those granted permission. All access permission questions should be directed to the database administrator of your organization.

The following are the hardware and software requirements for the Risk Assessment Database:

Pentium® 4 or equivalent processor

Windows XP

MS Access® 2002

256 MB of RAM recommended for all components

BEFORE USING THE DATABASE: ACCESS TO THE MANAGER'S VERSION OF THE RISK ASSESSMENT DATABASE

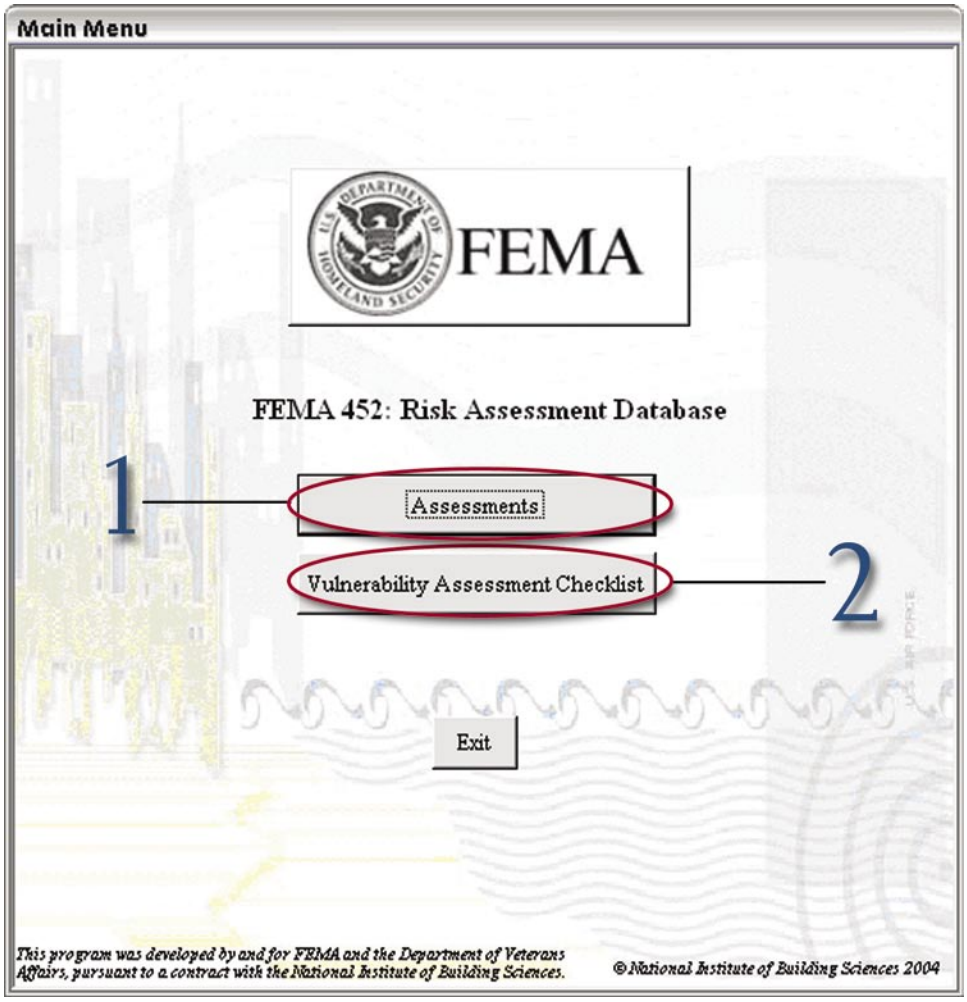
From your database administrator, the user should receive an application shortcut with the icon

- The ***application shortcut*** should be copied to the ***desktop***. When the user double clicks the application shortcut, the user receives a logon screen

  The user should log on using the user name and password provided by the database administrator.

- After logging on, the user will get the **Main Menu**.

MAIN MENU

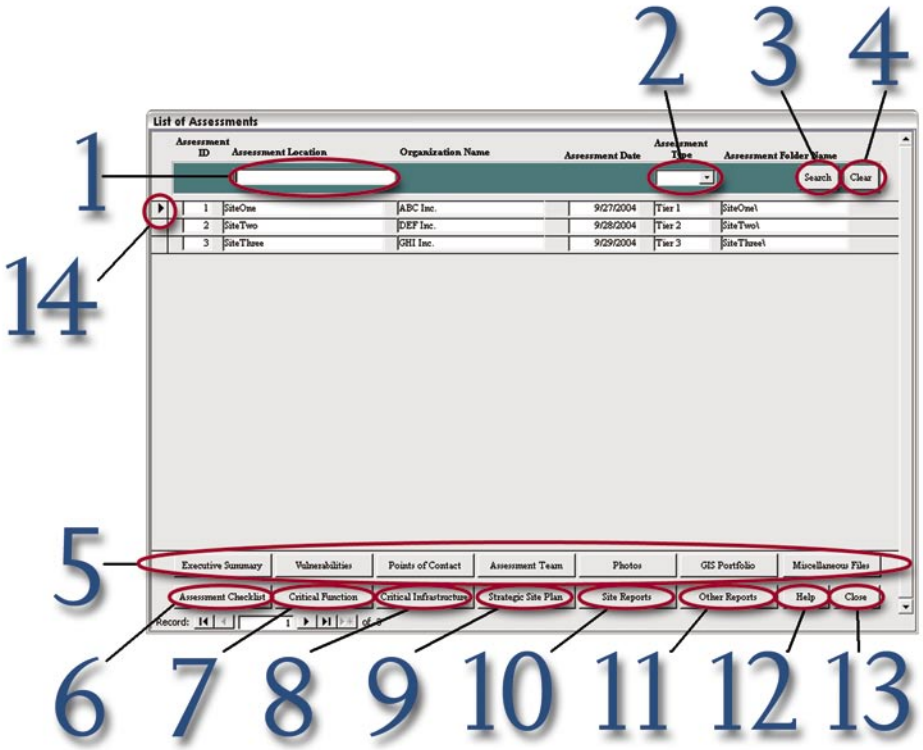


On startup, the Risk Assessment Database **Main Menu** displays two areas to navigate within the program. Select the ***Assessments*** button to view the risk assessment related information.

1. The ***Assessment*** button opens the **List of Assessments** form and all functionality included.

2. The ***Vulnerability Assessment Checklist*** button opens the **Assessment Checklist Question Details** form and all the functionality included.

LIST OF ASSESSMENTS



1. ***Assessment Location*** field allows for manual entry of full or partial station name for search.

2. ***Assessment Type*** field is a drop down menu to search for assessment type: Tier 1, 2, or 3.

3. ***Search*** button performs search based on criteria entered into the fields described above.

4. ***Clear*** (show all records) button will allow all sites to be seen again.

5. These buttons ***(Executive Summary, Vulnerabilities, Points of Contact, Assessment Team, Photos, GIS Portfolio, and Miscellaneous Files)*** open the **Assessment Main Page**.

6. The ***Assessment Checklist*** button opens the **Assessment Checklist** form.

7. The ***Critical Function*** button opens the **Critical Functions Matrix** form.

8. The ***Critical Infrastructure*** button opens the **Critical Infrastructure Matrix** form.

9. The ***Strategic Site Plan*** button opens the **Strategic Site Plan** in Microsoft Excel.

10. The ***Site Reports*** button opens the **Site Assessments Report** page.

11. The ***Other Reports*** button opens the **Keyword Search Reports Menu**.

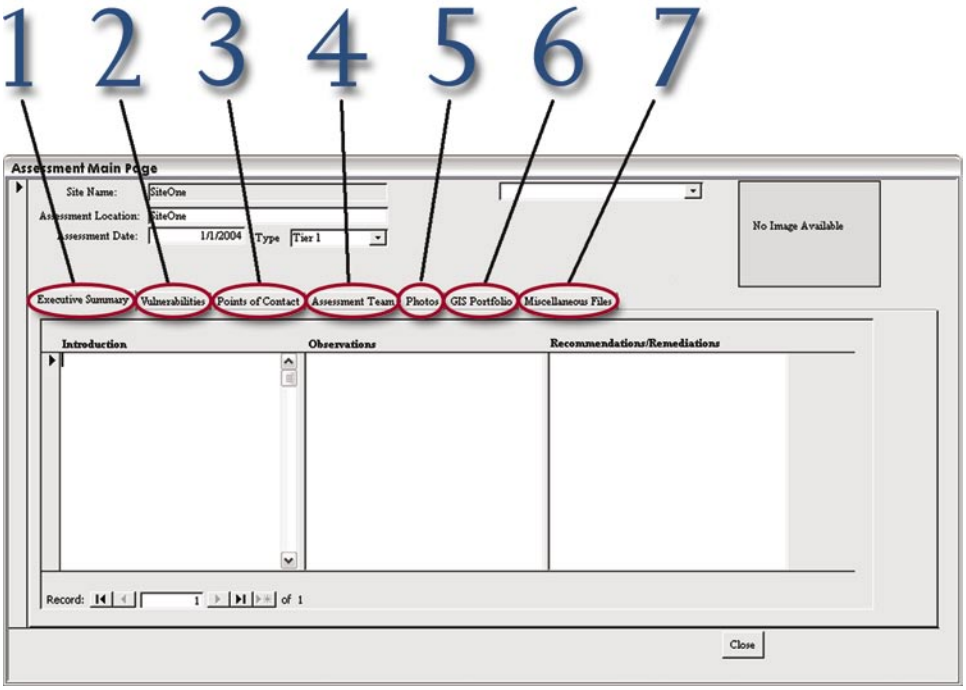
12. The ***Help*** button opens a window telling the user to press F1 for help. By pressing F1, this User Guide will open on your computer.

13. The ***Close*** button simply closes the **List of Assessments** page and returns to the **Main Menu**.

14. The black triangle indicates the record that is selected.

ASSESSMENT MAIN PAGE

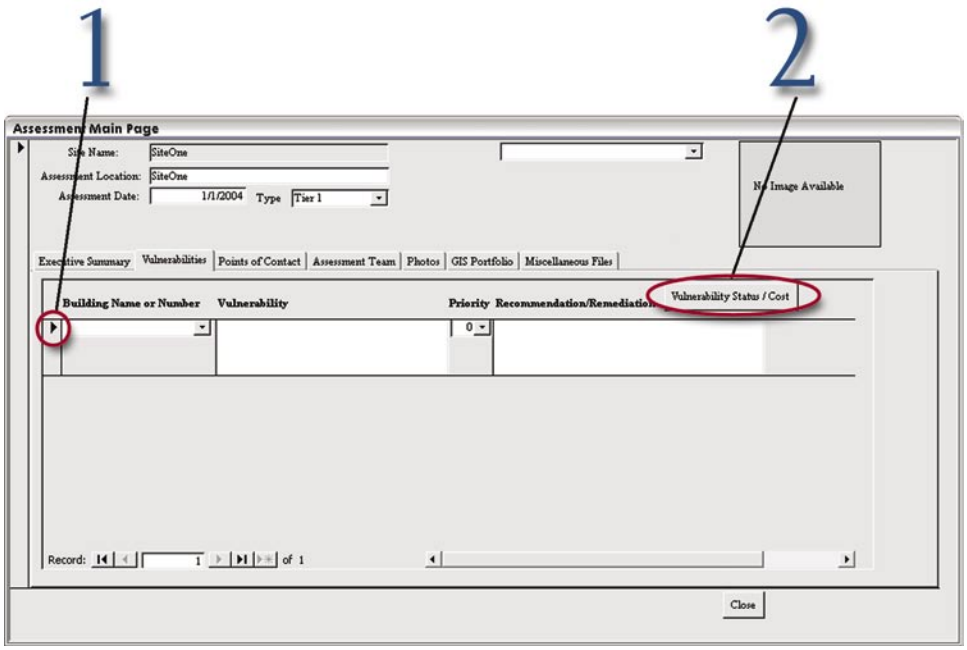
Executive Summary



This form allows the user to enter an Executive Summary for the assessment site report.

1. For the station selected in the **List of Assessments** form, this tab will show the ***Executive Summary*** entered by the Assessment Team.
2. For the station selected in the **List of Assessments** form, this tab will show the various ***Vulnerabilities*** for facilities at the designated site for that particular assessment.
3. For the station selected in the **List of Assessments** form, this tab will show the contact Information for the site points of contact ***(Points of Contact)***.
4. For the station selected in the **List of Assessments** form, this tab will show the contact information for the team that performed the assessment ***(Assessment Team)***.
5. For the station selected in the **List of Assessments** form, this tab will show the Photos collected during the assessment ***(Photos)***.
6. For the station selected in the **List of Assessments** form, this tab will show the GIS Portfolio for the assessment site ***(GIS Portfolio)***.
7. For the station selected in the **List of Assessments** form, this tab will show any other files that may be associated with the assessment site ***(Miscellaneous Files)***.

Vulnerabilities

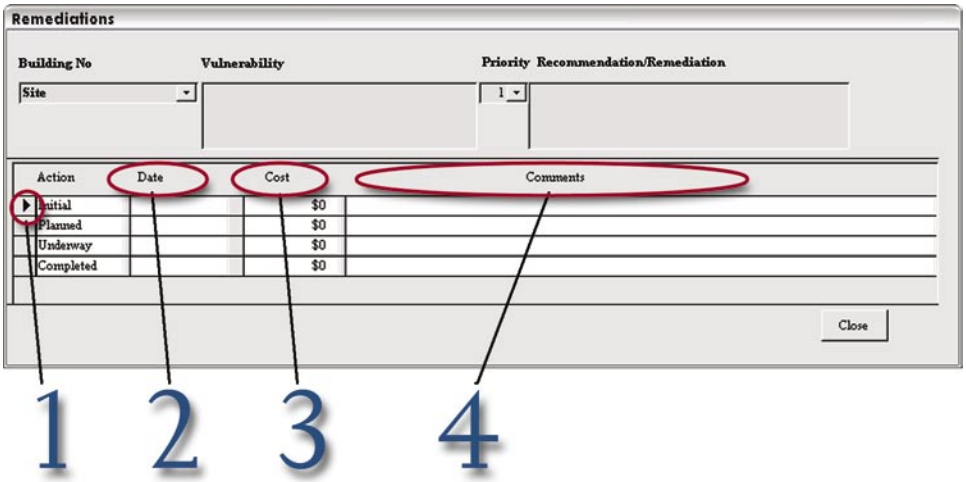


This form allows the user to view vulnerabilities and recommendations/remediations observed while performing the assessment. Note: Priority and Building Number are required.

1. The black triangle indicates the record that is selected.

2. The ***Vulnerability Status/Cost*** button opens the **Remediations** form and allows you to record cost data associated with the remediation of the selected vulnerability.

Remediations



This form allows the user to record cost data associated with the remediation of the selected vulnerability. The total cost of entries is reflected in other forms containing cost references.

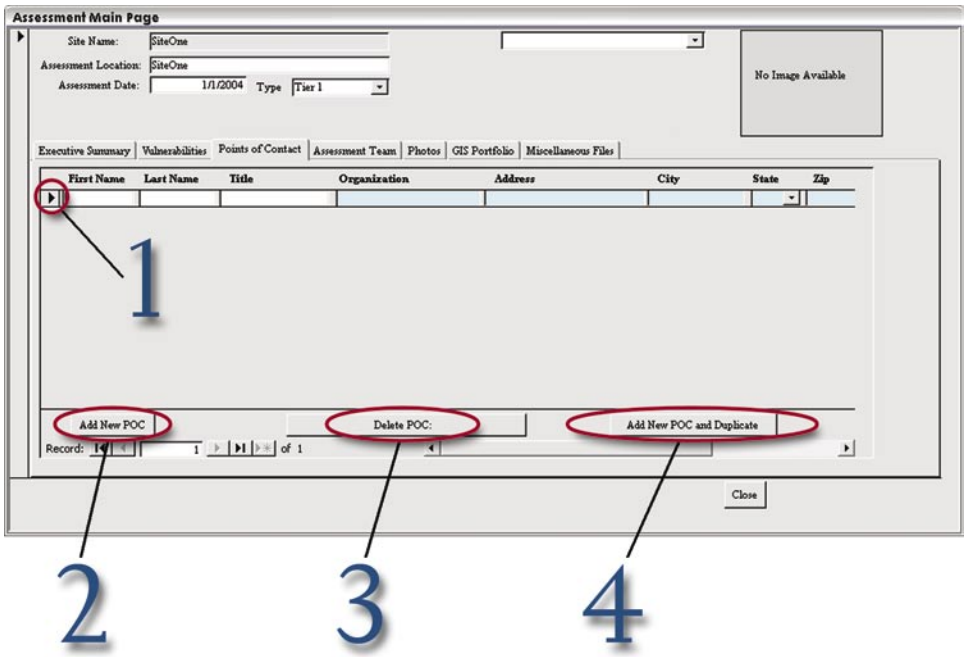
1. The black triangle indicates the record that is selected.

2. This field can be filled in by the user to track entries.

3. Enter the cost for the remediation into this field to keep the remediation records up to date.

4. Enter any comments for the remediation in this field.

Points of Contact



This form allows the user to view information about points of contact at the assessment site.

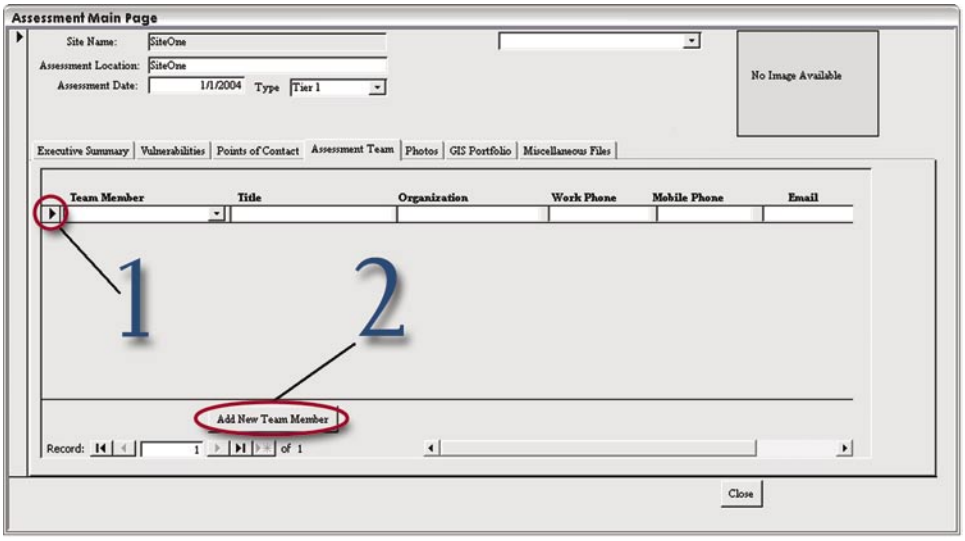
1. The black triangle indicates the record that is selected.

2. The ***Add New POC*** button allows for the creation of a new contact for the assessment site designated in the upper left portion of this form.

3. The ***Delete POC***: **(CONTACT NAME)** button allows the removal of the selected contact from the database.

4. The ***Add New POC and Duplicate*** button allows the creation of a new contact and duplicates the information in light blue in order to minimize data entry efforts.

Assessment Team

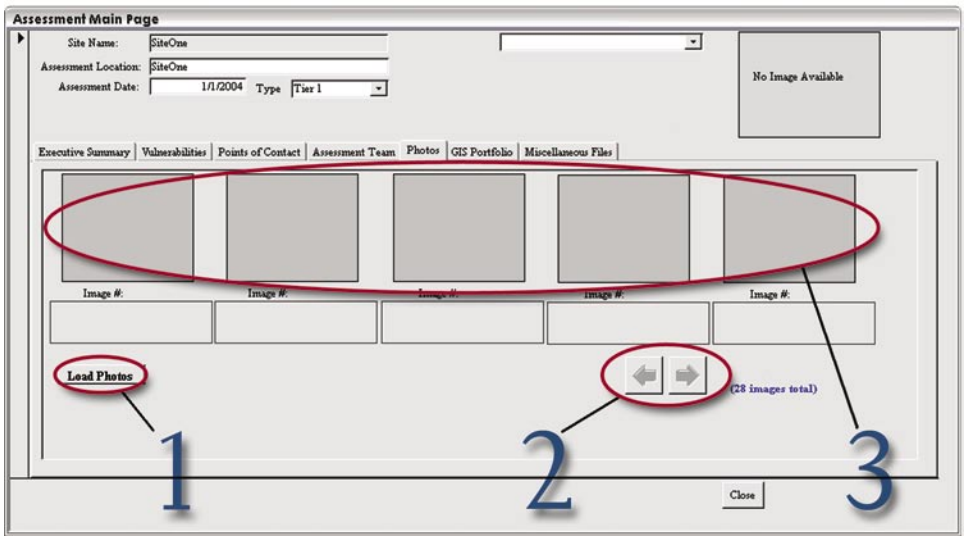


This form allows the user to view information about Assessment Team members.

1. The black triangle indicates the record that is selected.

2. The ***Add New Team Member*** button allows for the creation of a new Assessment Team member for the assessment site designated in the upper left portion of this form.

Photos

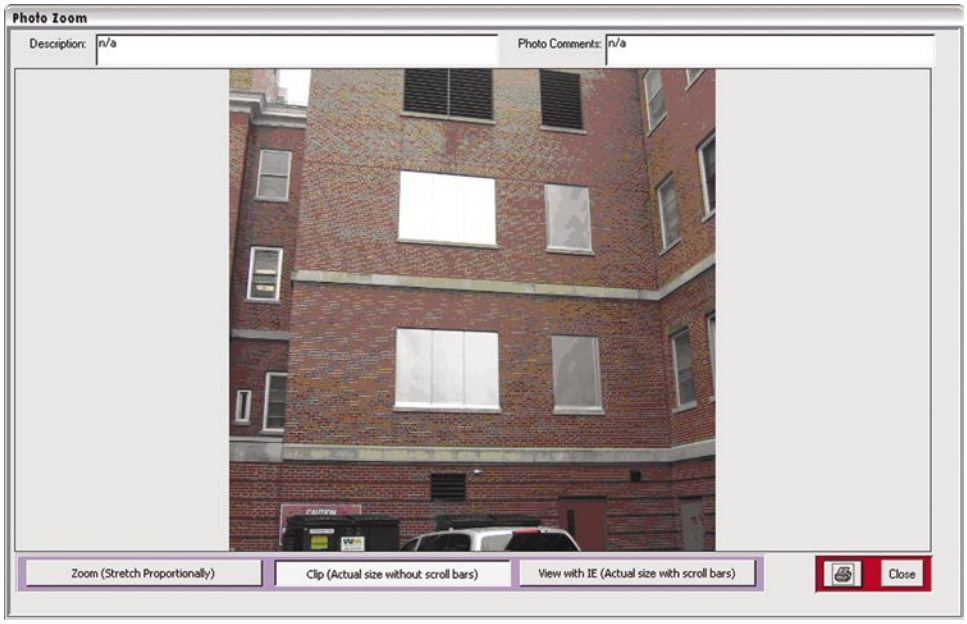


The user is able to see the photos associated with the assessment site on this form.

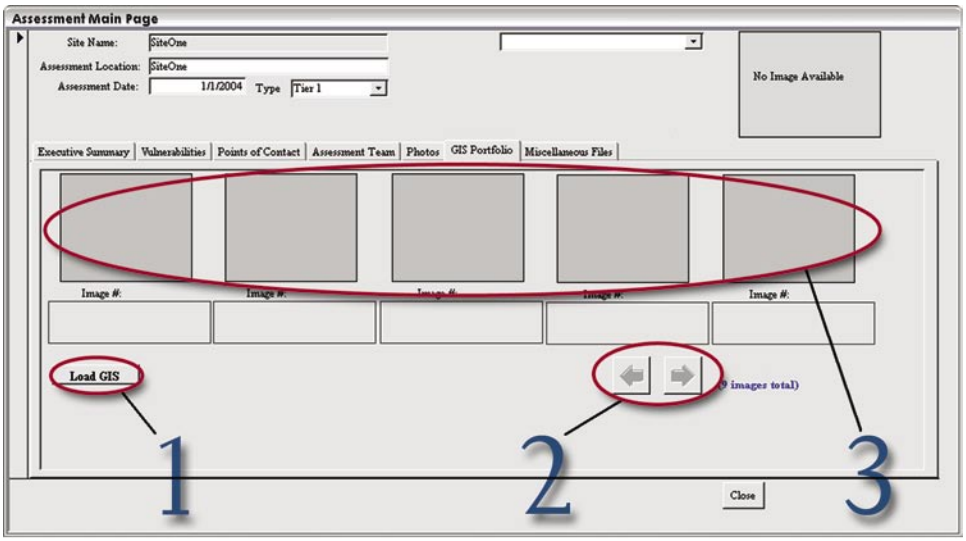
1. The ***Load Photos*** button loads photos into the designated frames.

2. The 2 arrow buttons allow for navigation through pages of 5 photos, either to the previous 5 photos or to the next 5 photos.

3. Clicking on any of the photos will open the photo in the ***Photo Zoom*** window, which displays the photo larger, and photos can be printed individually in this window.



GIS Portfolio



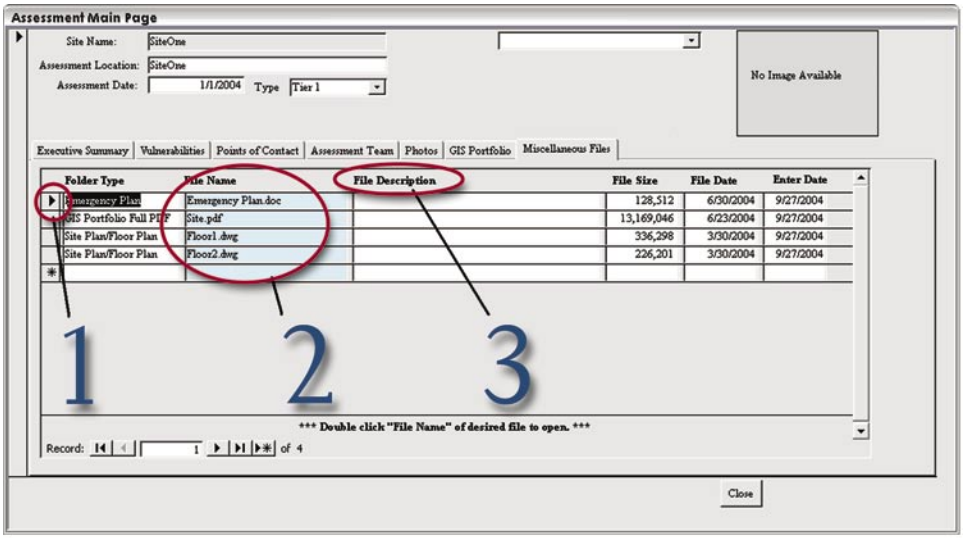
The user is able to see all GIS images associated with the assessment site on this form.

1. The ***Load GIS*** button loads GIS images to the designated frames.

2. The 2 arrow buttons allow for navigation through pages of 5 GIS images, either to the previous 5 images or to the next 5 images.

3. Clicking on any of the GIS images will open the image in the ***Photo Zoom*** window, which displays the image larger, and images can be printed individually in this window.

Miscellaneous Files



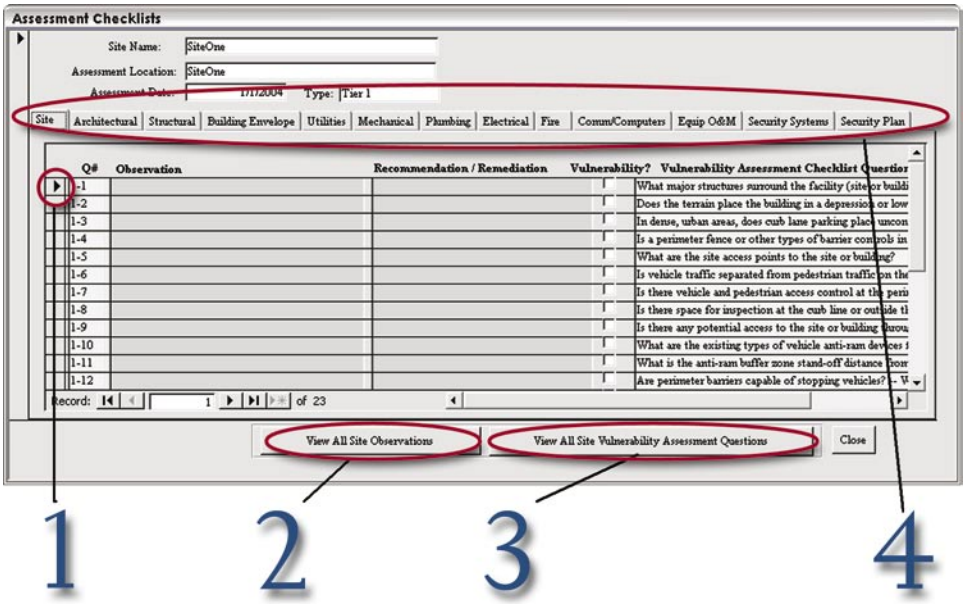
This form enables the user to see files related to the assessment that are available to view. The user can also open these files from this form.

1. The black triangle indicates the record that is selected.

2. Double-clicking in any of the filenames will open the associated file. (Examples of possible files to pre-load for the assessors include references, a GIS portfolio in PDF format, and/or past assessment reports.)

3. The ***File Description*** field allows for descriptions to be typed in about each of the file names in the record.

ASSESSMENT CHECKLISTS



This form shows an abbreviated entry for each of the questions under the category selected in the row of tabs under the assessment information section at the top of this form.

1. The black triangle indicates the record that is selected.

2. The ***View All Site Observations*** button allows the user to view all of the assessment checklist data (observations and recommendations/ remediations) for the selected section tab.

3. The ***View All Site Vulnerability Assessment Questions*** button allows the user to view all of the assessment checklist questions for the selected section tab.

4. These tabs represent a section in the assessment checklist. The user can select any of the tabs and have access to the assessment data in that section.

CRITICAL FUNCTIONS MATRIX

This form records and numerically displays the results of analysis performed during the assessment. The matrix lists Critical Functions down the left side and threats across the top to create Threat-pairs. For each Threat-pair, a numeric value, on a 1-10 scale, is recorded for a threat rating, an asset value rating, and a vulnerability rating. The methodology for determining the ratings is found in FEMA 452.

1. The black triangle indicates the record that is selected.

2. The ***Rollup*** button opens a window that summarizes all of the risk columns into one easy to read form called **Critical Functions Rollup**.

Critical Functions Rollup

1

Critical Functions Rollup

Site Name: SiteOne

Assessment Date: 01/01/2004

Assessment Type: Tier 1

Low Risk (1-60)
Medium Risk (61-175)
High Risk (>175)

No.	Critical Function	IED (Bomb) Risk	Chem Agent Risk	Arson/ Incend. Risk	Armed Attack Risk	Bio Agent Risk	Cyber-terrorism Risk	Agri-terrorism Risk	Radio-logical Risk	Nuclear Device Risk	Hazmat Release Risk	Unauth. Entry Risk	Surveil-lance Risk	Suicide Bomber Risk	Other CF-1 Risk	Other CF-2 Risk
1	Administration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Engineering	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Warehousing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Data Center	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Food Service	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Security	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Housekeeping	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Day Care	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Other CF-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	Other CF-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Other CF-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Other CF-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Other CF-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Other CF-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Other CF-7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Other CF-8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Other CF-9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Other CF-10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

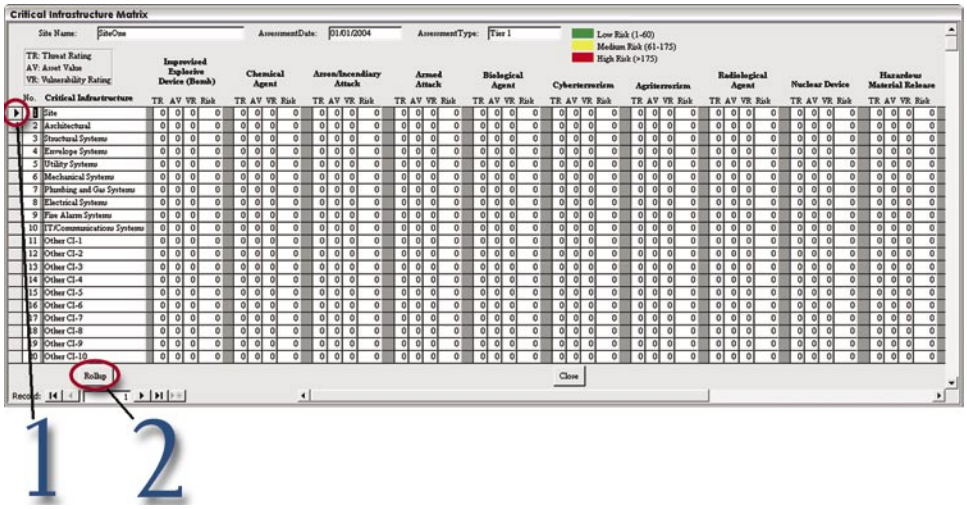
Close

Record: 1

This form displays a summary of the final numeric risk value of each Threat-pair in the **Critical Functions Matrix**.

1. The black triangle indicates the record that is selected.

CRITICAL INFRASTRUCTURE MATRIX



This form records and numerically displays the results of analysis performed during the assessment. The matrix lists Critical Infrastructure down the left side and threats across the top to create Threat-pairs. For each Threat-pair, a numeric value, on a 1-10 scale, is recorded for a threat rating, an asset value rating, and a vulnerability rating. The methodology for determining the ratings is found in FEMA 452.

1. The black triangle indicates the record that is selected.

2. The ***Rollup*** button opens a window that summarizes all of the risk columns into one easy to read form called **Critical Infrastructure Rollup**.

Critical Infrastructure Rollup

Critical Infrastructure Rollup

Site Name: SiteOne
Assessment Date: 01/01/2004
Assessment Type: Tier 1

Low Risk (1-60)
Medium Risk (61-175)
High Risk (>175)

No.	Critical Infrastructure	IED (Bomb) Risk	Chem Agent Risk	Arson/ Incend. Risk	Armed Attack Risk	Bio Agent Risk	Cyber-terrorism Risk	Agri-terrorism Risk	Radio-logical Risk	Nuclear Device Risk	Hazmat Release Risk	Unauth. Entry Risk	Surveil-lance Risk	Suicide Bomber Risk	Other CI-1 Risk	Other CI-2 Risk
1	Site	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Architectural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Structural Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Envelope Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Utility Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Mechanical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Plumbing and Gas Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Electrical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Fire Alarm Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	IT/Communications Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Other CI-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Other CI-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Other CI-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Other CI-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Other CI-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Other CI-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Other CI-7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Other CI-8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	Other CI-9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	Other CI-10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Close

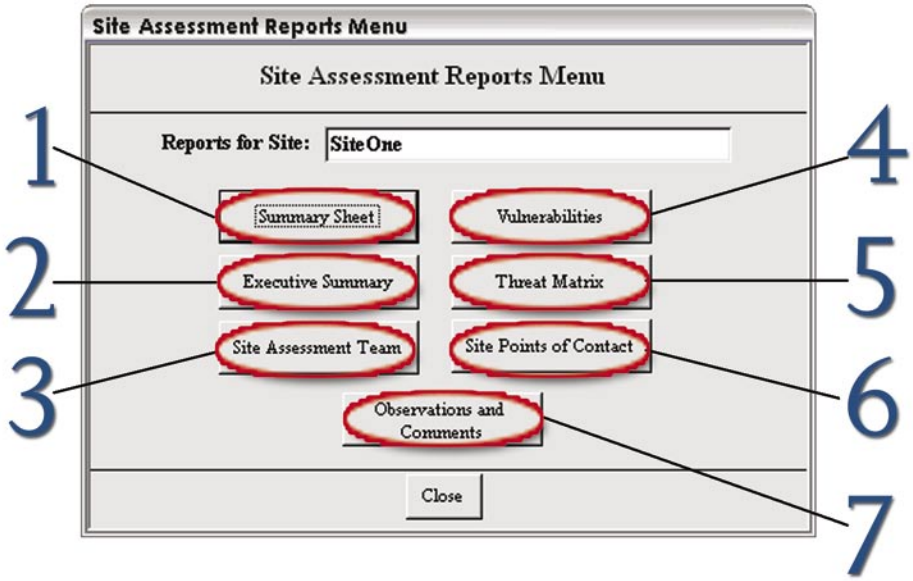
Record: 1 of 20 (Filtered)

1

This form displays a summary of the final numeric risk value of each Threat-pair in the **Critical Infrastructure Matrix**.

1. The black triangle indicates the record that is selected.

SITE ASSESSMENT REPORTS MENU



This menu is displayed when selecting the ***Site Reports*** button on the **List of Assessments** main form. From this location, the user can print any of the automated reports for the assessment specified at the top of the menu (the selected record on the **List of Assessments** for when the ***Site Reports*** button was depressed).

1. The ***Summary Sheet*** button produces the **Site Summary Sheet** report.

2. The ***Executive Summary*** button produces the **Executive Summary** report.

3. The ***Site Assessment Team*** button produces the report listing the information for the individual assessors responsible for that particular assessment.

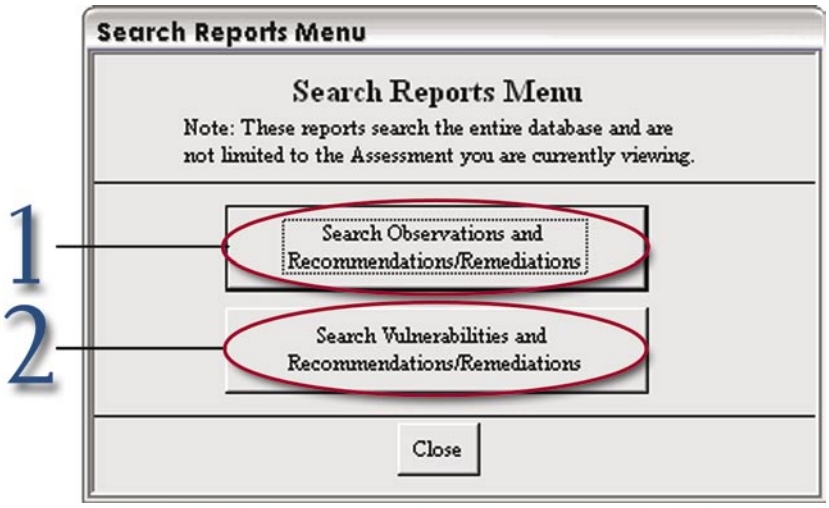
4. The ***Vulnerabilities*** button opens the produces the **Vulnerabilities and Recommendations/Remediations** report.

5. The ***Threat Matrix*** button will perform an automated process that opens an Microsoft document and then populates the information for both the **Critical Functions Matrix** and the **Critical Infrastructure Matrix**.

6. The ***Site Points of Contact*** button produces the **Site Point of Contacts** report.

7. The ***Observations*** and ***Comments*** button creates the **Assessment Observations and Comments** report.

KEYWORD SEARCH REPORTS MENU



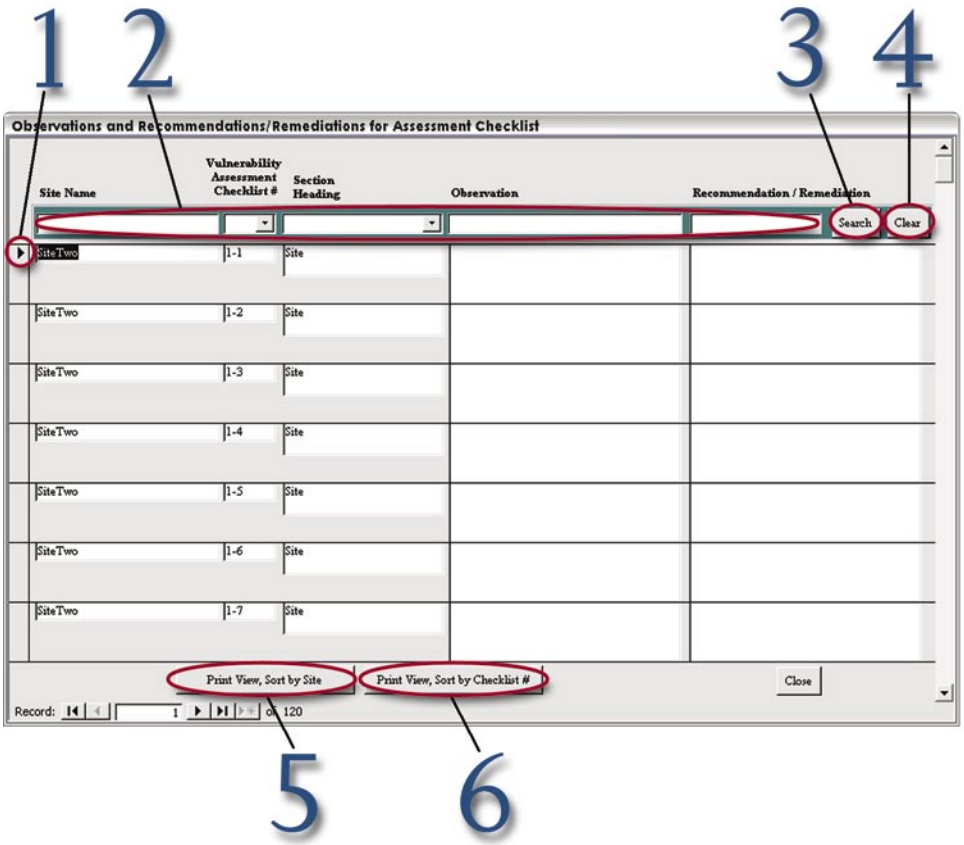
This menu appears after the user selects the ***Other Reports*** button at the bottom of the **List of Assessments** form.

1. The ***Search Observations*** and ***Recommendations/Remediations*** button opens the **Observations and Recommendations/Remediations for Assessment Checklist** form.

2. The ***Search Vulnerabilities*** and ***Recommendations/Remediations*** button opens the **Vulnerabilities** and **Recommendations/Remediations** form.

Note: these reports search the entire database and are not limited to the assessment the user is currently viewing.

Observations and Recommendations/Remediations for the Assessment Checklist



This form is used to search all the observations and recommendations/remediations for all the assessment sites.

1. The black triangle indicates the record that is selected.

2. The fields in the green box allow the user to search for and display only the observations and recommendations/remediations of interest.

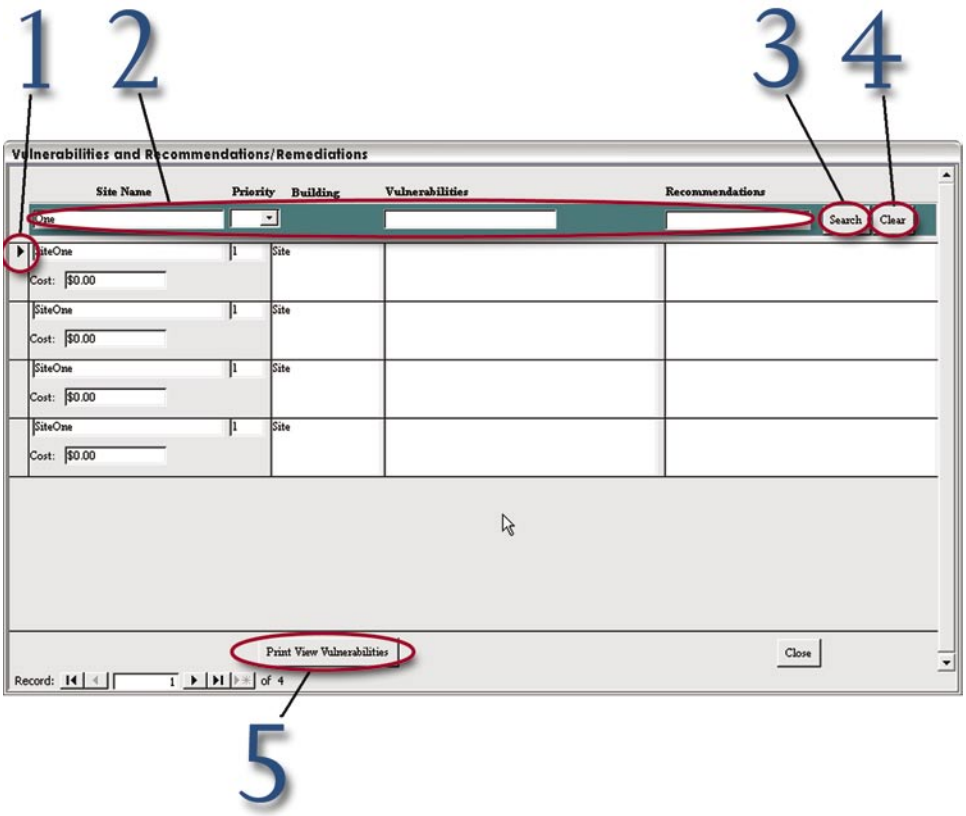
3. The ***Search*** button performs search based on criteria entered into the fields described above.

4. The ***Clear*** (show all records) button will allow all sites to be seen again.

5. The ***Print View, Sort by Site*** button will create a report of the search results sorted by site name.

6. The ***Print View, Sort by Checklist #*** button will create a report of the search results sorted by the question number.

Vulnerabilities and Recommendations/Remediations



This form is used to search all the vulnerabilities and recommendations/remediations for all the assessment sites.

1. The black triangle indicates the record that is selected.

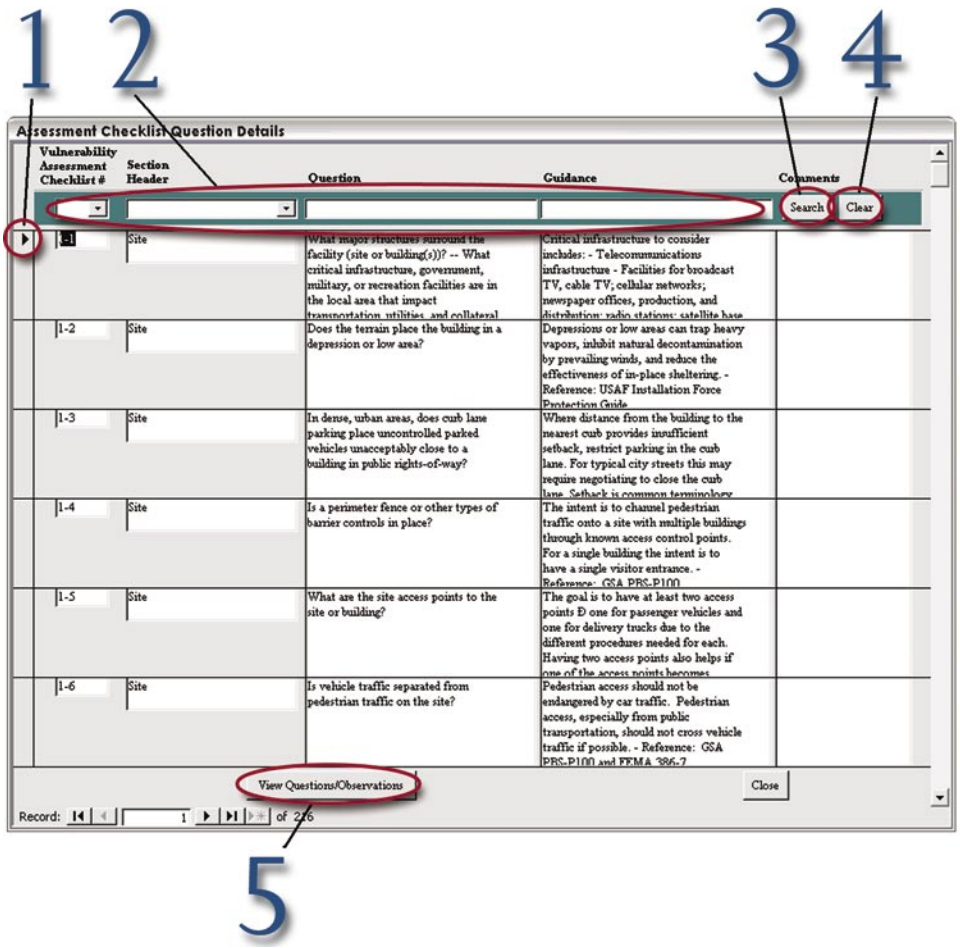
2. The fields in the green query box allow the user to search for and display only the vulnerabilities and recommendations/remediations of interest.

3. The ***Search*** button performs search based on criteria entered into the fields described above.

4. The ***Clear*** (show all records) button will allow all sites to be seen again.

5. The ***Print View Vulnerabilities*** button will create a report of the **Search** results.

ASSESSMENT CHECKLIST QUESTION DETAILS



This form shows all of the vulnerability assessment checklist questions in the database.

1. The black triangle indicates the record that is selected.

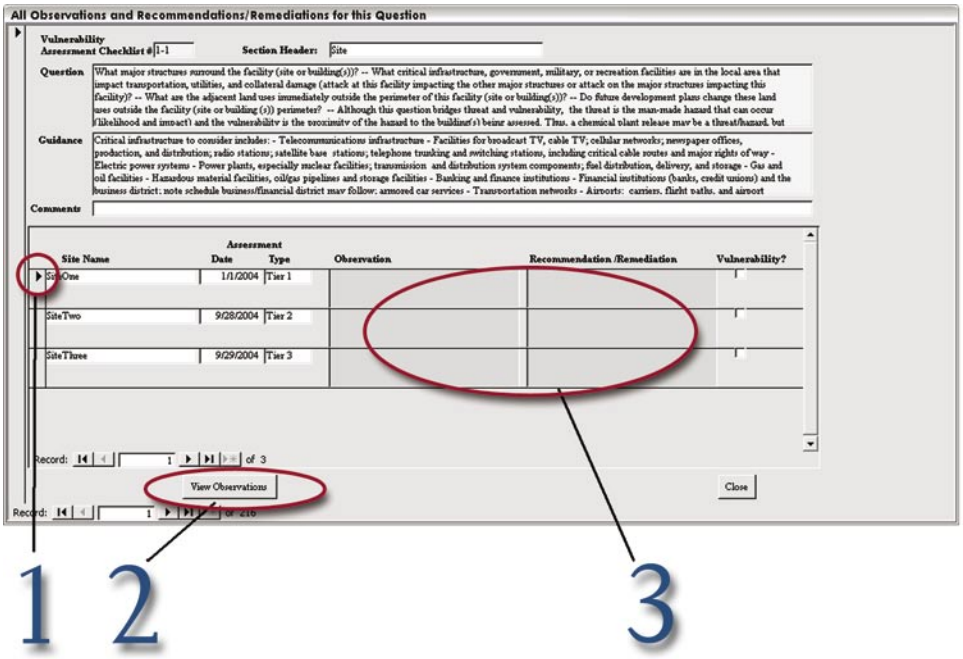
2. The green query bar allows the user quick access to the assessment questions by utilizing a drop down menu to select the question numbers or section header. There are also manually entered search forms for Question or Guidance by searching for keywords entered.

3. The ***Search*** button performs search based on criteria entered into the fields described above.

4. The ***Clear*** (show all records) button will allow all sites to be seen again.

5. The ***View Questions/Observations*** button opens the **All Observations and Comments for This Question** for the selected question.

All Observations and Recommendations/ Remediations for This Question



This form provides the user with all database entries for the question selected in the **Assessment Checklist Question Details** form when the ***View Questions/ Observations*** button was selected. It displays the questions, guidance, and comments at the top of the form. The bottom of the form displays all information entered for that specific question number.

1. The black triangle indicates the record that is selected.

2. The ***View Observations*** button creates a report of all entries in the database for the designated question.

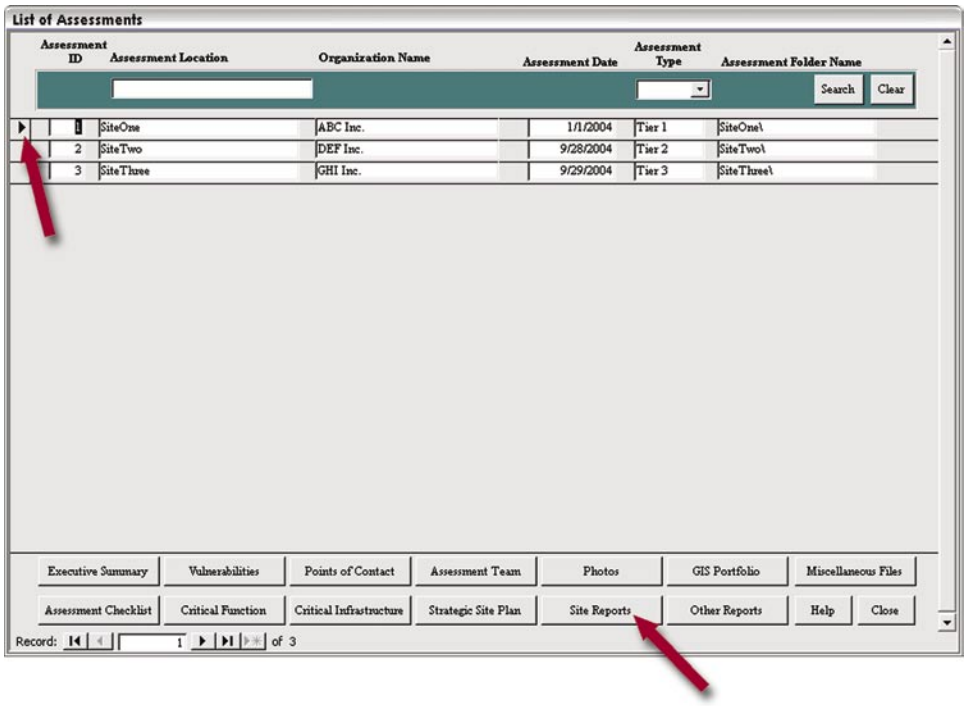
3. Double clicking on the ***View Observations*** or ***Recommendation/Remediation*** fields will open a form that allows the user to change the assessment data for the record.

PRINTING REPORTS AND ACCOMPANYING MATERIALS

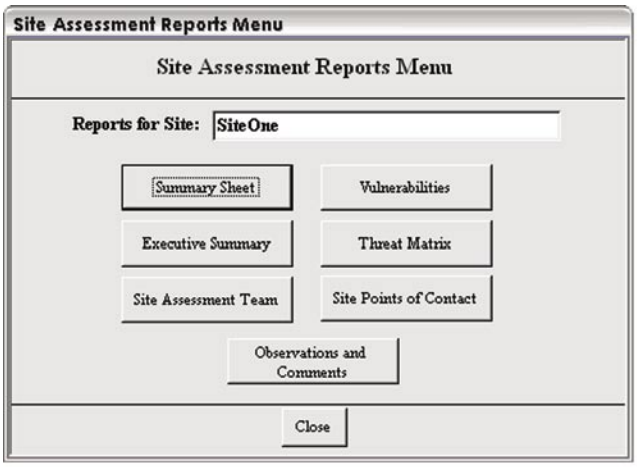
Printing Assessment Sections Completed by Assessors

1. Open the database, and click on the ***Assessments*** button.

2. The **List of Assessments** window will open. Place the arrow on the left next to the desired assessment site. Click on the ***Site Reports*** button.



3. The **Site Assessment Reports Menu** window will appear for the selected assessment site.

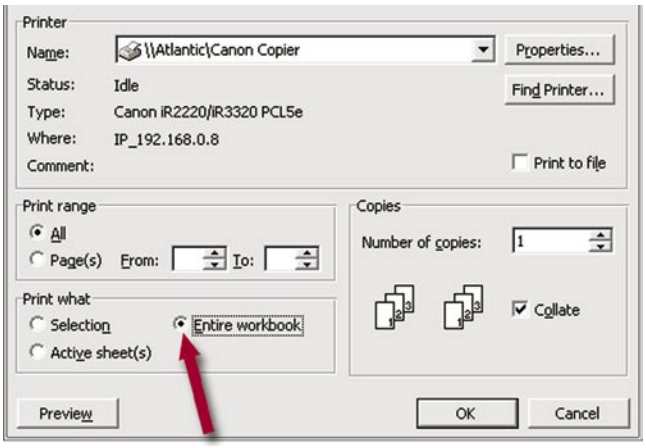


a. Clicking on the ***Summary Sheet, Executive Summary, Site Assessment Team, Vulnerabilities, Threat Matrix, Site Points of Contact,*** or ***Observations and Comments*** button will produce an onscreen report, which can then be printed for a hard copy of that section.

b. The sections that are normally used in an assessment report are the ***Executive Summary, Site Assessment Team, Vulnerabilities, Threat Matrix,*** and ***Site Points of Contact***.

c. The ***Threat Matrix*** button will produce a formatted Microsoft Excel Book with values.

d . To print both matrices (Functions and Infrastructure), go to File → Print (in Excel), and be sure to select ***"Entire workbook"*** before clicking ***"OK"***.



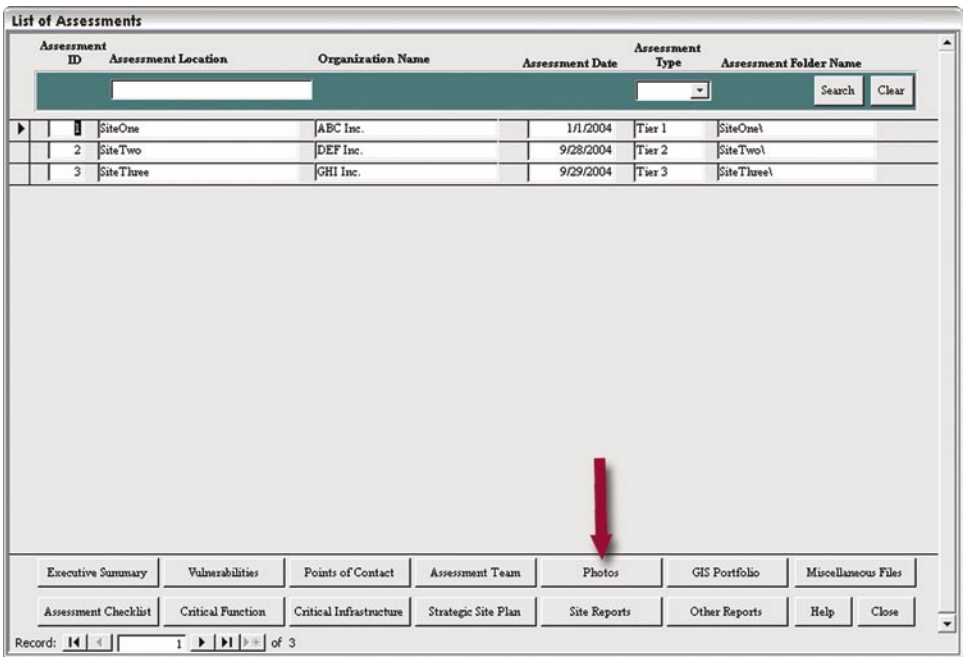
4. Print desired sections.

5. Close the **Site Assessment Reports Menu** to return to the **List of Assessments** window.

Printing Photos, GIS Portfolio, Floor Plans, Emergency Plans, and Other Related Documents

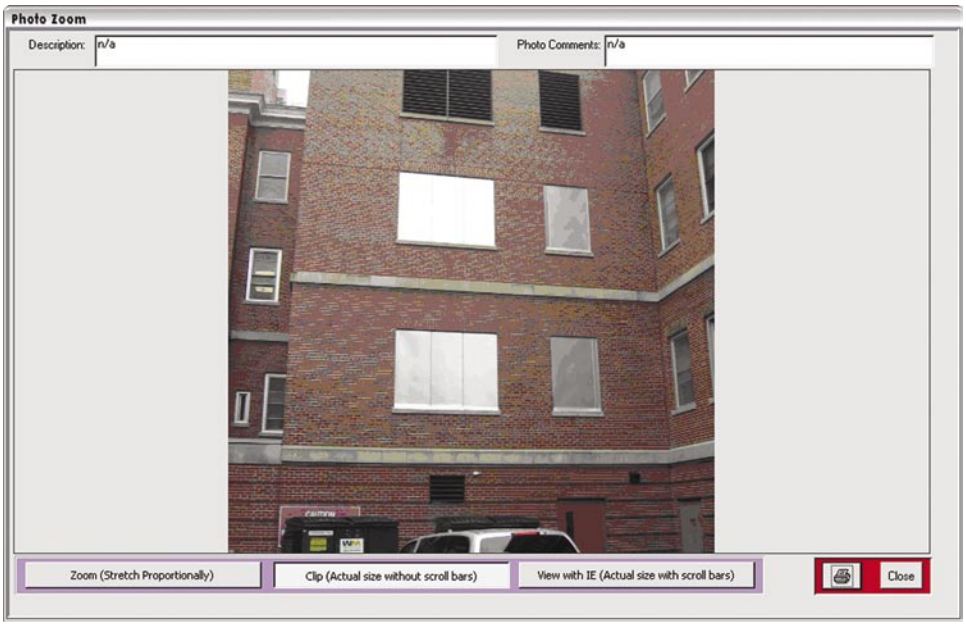
Printing Photos

1. On the **List of Assessments** window, click the ***Photos*** button.



2. The **Assessment Main Page** window will open, and the ***Photos*** tab will be open. Click ***Load Photos*** to display the photos.

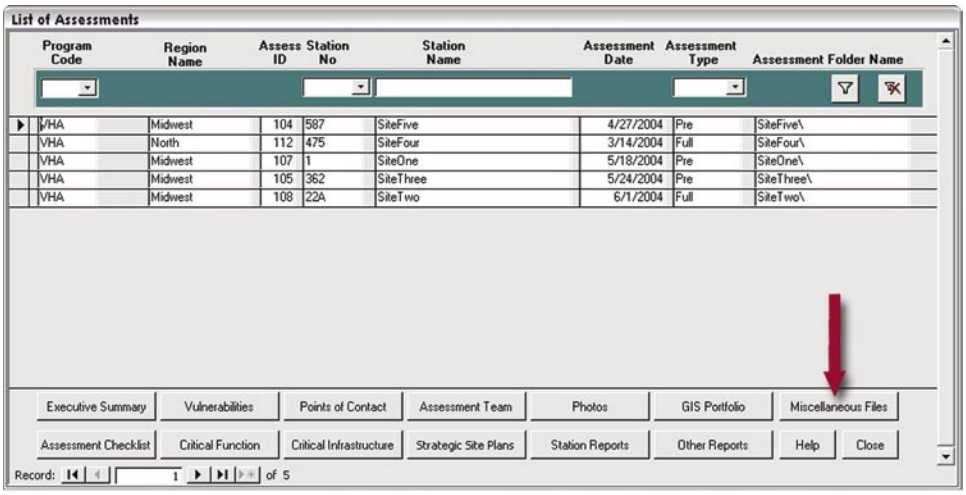
3. To open a photo for printing, double click on the thumbnail for the desired photo, and a **Photo Zoom** window will open:



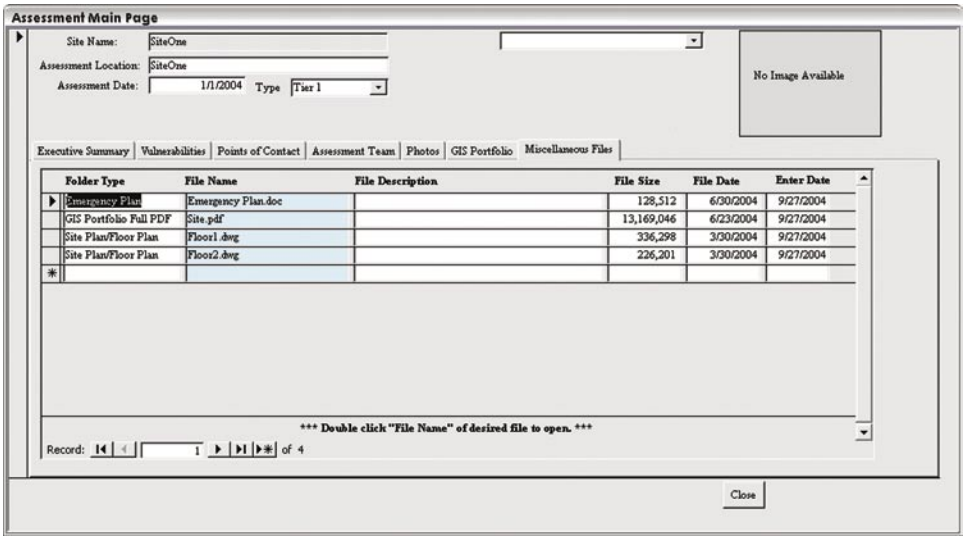
4. Close the **Photo Zoom** window and the **Assessment Main Page** window to return to the **List of Assessments** window.

Printing GIS Portfolio, Floor Plans, Emergency Plans, and Related Documents

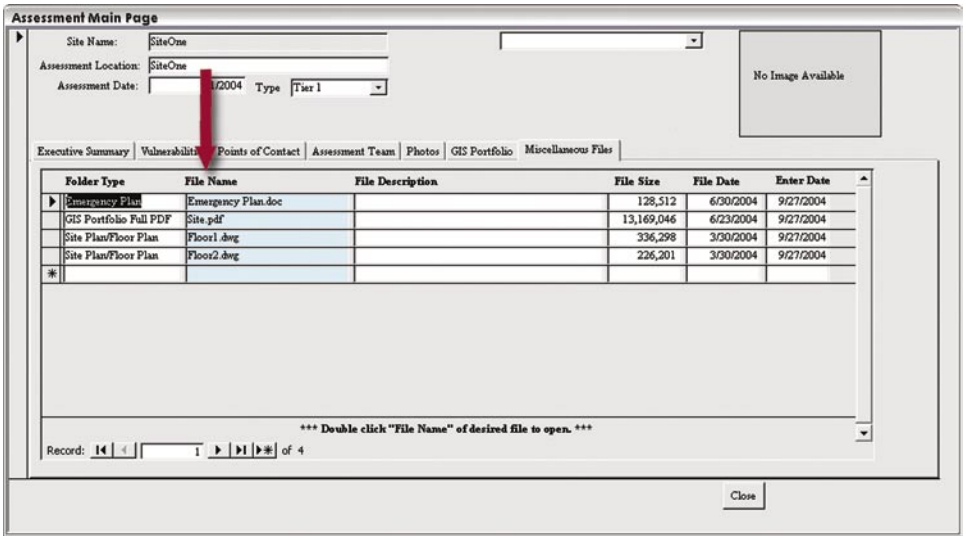
1. On the **List of Assessments** window, click the ***Miscellaneous Files*** button.



2. The **Assessment Main Page** window will open, and the ***Miscellaneous Files*** tab with those files loaded in the assessment will be displayed. This may be blank if no files were collected. For the User Guide we have listed 4 file examples:



3. To open the desired files, double click the ***File Name*** of the desired file.



Note: The desired files are designated by ***Folder Type***. GIS Portfolios, Floor Plans, Emergency Plans, and the other reports will each have a designated ***Folder Type***. Also, ***each file will open with a program external to the database. It is necessary that the program be installed on the computer to open the desired file.***

- The ***GIS Portfolio***, if part of the assessment, will have a Folder Type of ***GIS Portfolio Full PDF***. The file will open with ***Adobe Acrobat.*** (Download at: http://www.adobe.com/products/acrobat/readstep2.html)
- The ***Floor Plans*** will have a Folder Type of ***Site Plan/Floor Plan.*** These files will generally open with any ***AutoCAD viewer/reader (DWG),*** such as Volo View.
- The ***Emergency Plans*** will have a Folder Type of ***Emergency Plan.*** These files will generally open with ***Microsoft Word.***

4. Print each file from the program it opens in.

B

BCC	Backup Control Center

C

CAD	computer-aided design
CBR	chemical, biological, or radiological
CCTV	closed-circuit television
CDC	Centers for Disease Control and Prevention
CEMP	Certified Emergency Management Plan
CIA	Central Intelligence Agency
COG	Continuity of Government
COOP	Continuity of Operations
COTS	Commercial off the Shelf
CSI	Construction Specifications Institute

D

DHS	Department of Homeland Security
DoD	Department of Defense

E

EMS	Emergency Management Services
EOC	Emergency Operations Center
EPA	Environmental Protection Agency

F

FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency

G

GIS	Geographic Information System
GSA	General Services Administration

H

HazMat	hazardous material
HEMP	High-Altitude Electromagnetic Pulse
HPM	High Power Microwave
HSO	Homeland Security Office
HSOC	Homeland Security Operations Center
HVAC	heating, ventilation, and air conditioning

I

IA/IP	Information Analysis and Infrastructure Protection
IP/TCP	Internet Protocol/Transmission Control Protocol
ISC	Interagency Security Committee
IT	information technology

J

JRIES	Joint Regional Information Exchange System

L

LAN	local area network
LEPC	Local Emergency Planning Committee

M

MOU	Memorandum of Understanding

N

NAVFAC	Naval Facilities Engineering Command
NIBS	National Institute of Building Sciences
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology

P

PC	personal computer
PPE	personal protective equipment
psi	pounds per square inch
RDD	radiological dispersal device

S

SBU	Sensitive-but-Unclassified
SERC	State Emergency Response Commission

T

TIC	Toxic Industrial Compound
TNT	trinitrotoluene
TTIC	Terrorist Threat Integration Center

U

UPS	uninterruptible power supply
USDA	U.S. Department of Agriculture

V

VA	Department of Veterans Affairs
VoIP	Voice over Internet Protocol

W

WAN	wide area network
WMD	weapons of mass destruction