Building Terrorism Mitigation - Vulnerability Assessment

Course No: F05-001

Credit: 5 PDH

Gilbert Gedeon, P.E.

Continuing Education and Development, Inc.
22 Stonewall Court
Woodcliff Lake, NJ 07677

P: (877) 322-5800
info@cedengineering.com

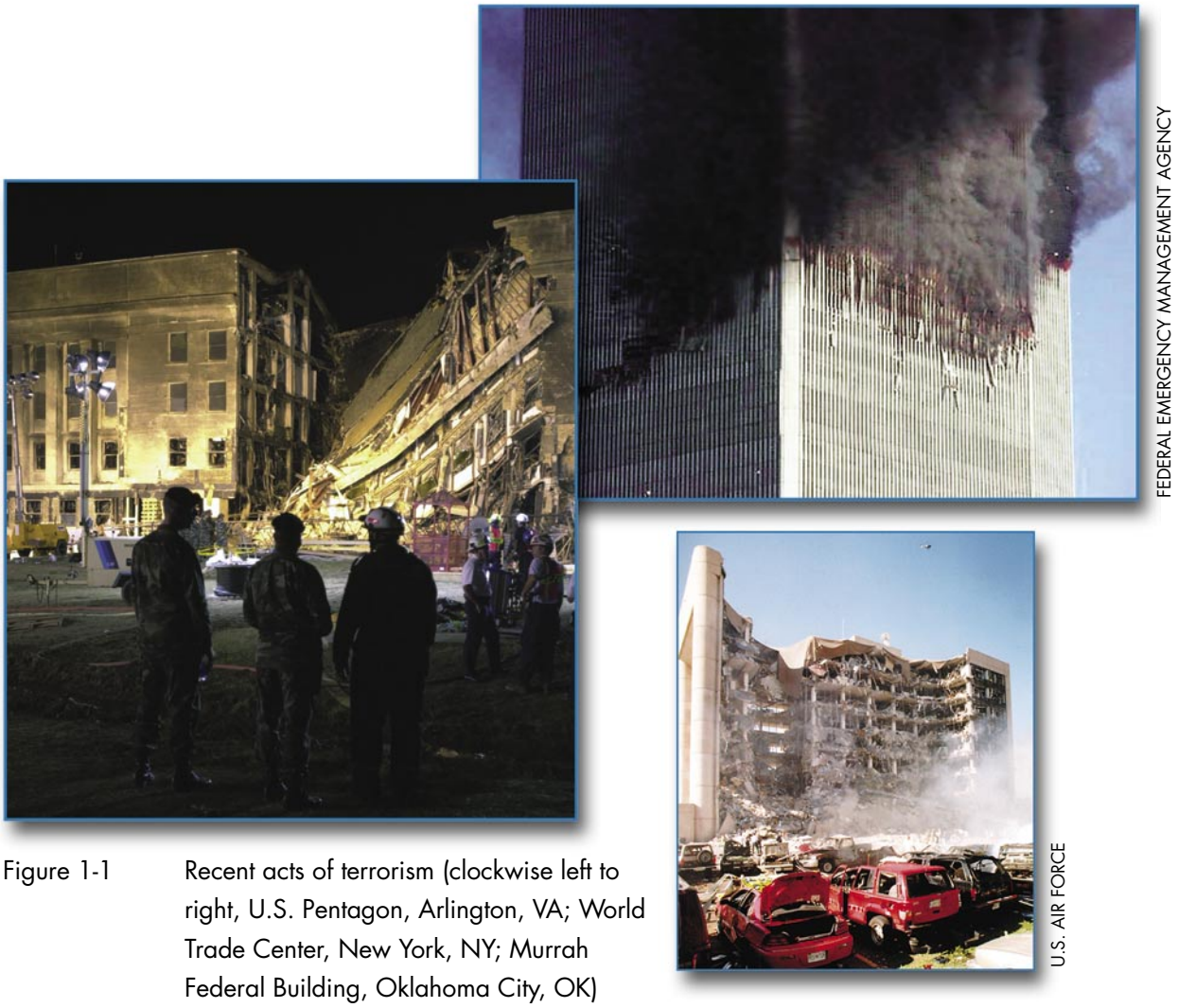
ASSET VALUE, THREAT/HAZARD, VULNERABILITY, AND RISK 1

Mitigating the threat of terrorist attacks against high occupancy buildings is a challenging task. It is difficult to predict how, why, and when terrorists may attack. Many factors must be considered in creating a safe building environment. This chapter presents several methodologies for architects and engineers to quantify risk and to identify the most effective mitigation measures to achieve a desired level of protection against terrorist attacks at an acceptable cost. The methodologies presented herein can be used for new buildings during the design process, as well as for existing buildings undergoing renovation. Sections 1.1 to 1.5 will discuss the assessment process, asset value assessment, threat/hazard assessment, vulnerability assessment, risk assessment, and risk management to help architects and engineers identify the best and most cost-effective terrorism mitigation measures for each building's unique security needs. Section 1.6 presents the Building Vulnerability Assessment Checklist to support the assessment process.

One of the primary objectives of this manual is to establish a common framework of terminology and the transfer of design concepts that have been in use by the United States (U.S.) Department of Defense (DoD), military services, the Department of State (DOS), and the General Services Administration (GSA) to commercial practice. The beginning point is to establish a basis for design by identifying the threat or hazard to be designed against. Within the military services, intelligence community, and law enforcement, the term "threat" is typically used to describe the design criteria for terrorism or manmade disasters. Within the Federal Emergency Management Agency (FEMA) and other civil agencies, the term "hazard" is used 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." These are distinct from natural hazards primarily in that they originate from human activity. Furthermore, "technological hazards" are generally

assumed to be accidental and that their consequences are unintended. For the sake of simplicity, this manual will use the terms "threat" and "hazard" when referring to terrorism and manmade disasters, respectively.

Terrorism and physical attacks on buildings have continued to increase in the past decade. The geographical isolation of the United States is not a sufficient barrier to prevent an attack on U.S. cities and citizens. Figures 1-1 and 1-2 demonstrate the far-reaching incidents and diverse natures and targets of recent terrorist attacks.

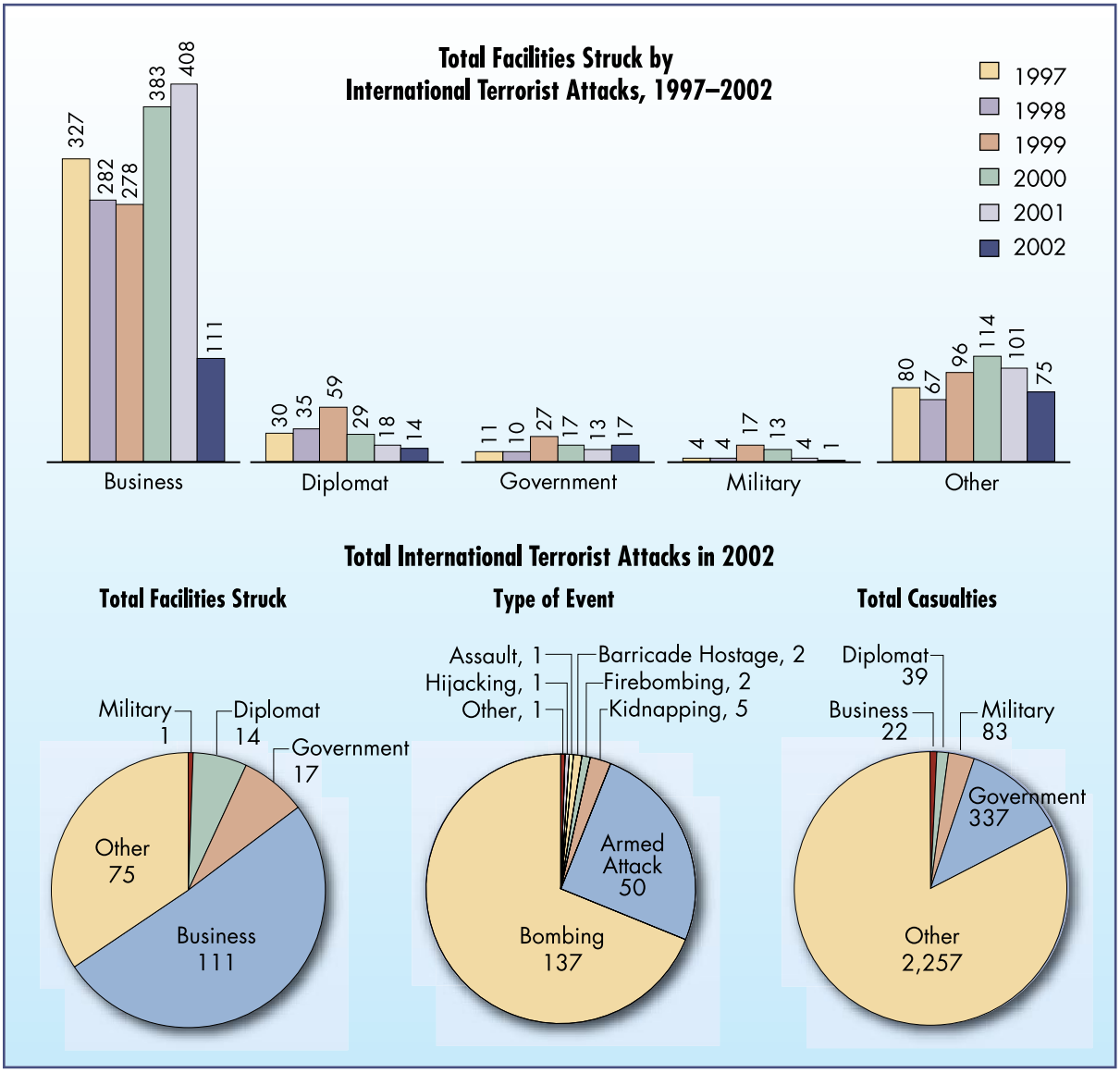


FEDERAL EMERGENCY MANAGEMENT AGENCY

FEDERAL EMERGENCY MANAGEMENT AGENCY

U.S. AIR FORCE

Figure 1-1 Recent acts of terrorism (clockwise left to right, U.S. Pentagon, Arlington, VA; World Trade Center, New York, NY; Murrah Federal Building, Oklahoma City, OK)



SOURCE: *DEPARTMENT OF STATE PATTERNS OF GLOBAL TERRORISM 2002*

Figure 1-2 Total facilities struck by international terrorist attacks in 1997-2002 and total facilities attacked in 2002

Design of buildings to survive natural hazards is a concept that is well understood by the design community. Many years of historical and quantitative data, and probabilities associated with the cycle, duration, and magnitude of natural hazards exist. Conversely, design of buildings that can survive the threat and impact of a terrorist attack is based on qualitative factors that evaluate organization requirements, recovery efforts and impacts, and loss

of personnel and infrastructure, but have no predictable period of recurrence or damage probability. Terrorist attacks are often categorized as low probability, but potentially high consequence, events. Building designs must include physical security measures as an integral part of the design process.

This chapter presents selected methodologies to determine asset value, analyze the threat/hazard, and evaluate vulnerabilities to complete the risk assessment. These elements of information become the input for determining relative levels of risk. Higher risk hazards may require more complex mitigation measures to reduce risk. Mitigation measures are conceived by the design professional and are best incorporated into the building architecture, building systems, and operational parameters, with consideration for life-cycle costs.

In order to create a safe environment, many factors must be considered. Figure 1-3 depicts the 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 part of the assessment process identifies the value of a building's assets (described in Section 1.1) that need to be protected. The second step is to conduct a threat assessment wherein the threat or hazard is identified, defined, and quantified (see Section 1.2). 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.

After conducting a threat assessment, the next step is to conduct a vulnerability assessment (see Section 1.3). 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

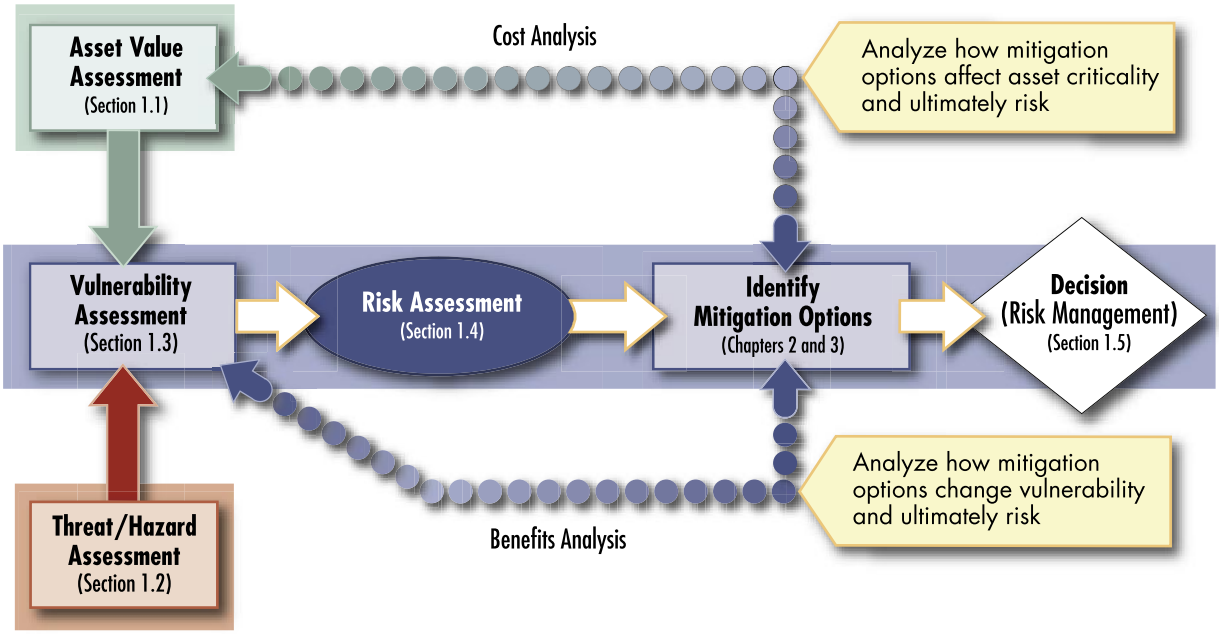


Figure 1-3 The assessment process model

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 (see Section 1.4). 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 identified vulnerability, allow prioritization of resources to implement mitigation measures.

When starting the design process for any new building or the renovation of an existing one, various owner, statutory, and building

use inputs are required. These inputs must be integrated to ensure that mandatory building code requirements are met, the building will meet the owner's functional needs, and natural and manmade hazards are mitigated to an acceptable level. In some cases, mitigation measures to enhance security may be in conflict with other design intentions. The assessment process helps to ensure an understanding of risk, so that it can be consciously addressed within the design process with available resources.

For natural hazards (earthquakes, grassland and forest fires, floods, and winds) and building fire hazards (technological accidents), information is available in building codes, industry standards, and FEMA guidelines. For manmade hazards, the suggested course of action is less well defined. The United States has not yet developed building standards similar to those of the United Kingdom, which has a greater history of contending with repeated terrorism on its home soil. Helpful information may be found in a strategic plan or a site master plan, or it may have to be developed during initial design through interviews with building owners, staff, occupants, utility companies, local law enforcement, and others.

There are many tools and techniques available to the designer for the development of new building designs, the renovation of existing buildings, and mitigation of vulnerabilities. Advances in commercial satellite imagery, Geographic Information Systems (GIS) (see Figures 1-4 and 1-5), structural hardening, glass fragmentation films, physical security systems, and many other building related technologies provide the design professional with numerous tools to design buildings to better protect occupants from terrorist acts.

Another challenge for the design team is to present appropriate information to the building owner/decision-maker in a manner that allows him or her to make a rational, informed decision. Ideally, design basis threats will be identified and agreed upon at the earliest stages of design (no later than preliminary design). The reason for this is twofold. First, the designer must have a known

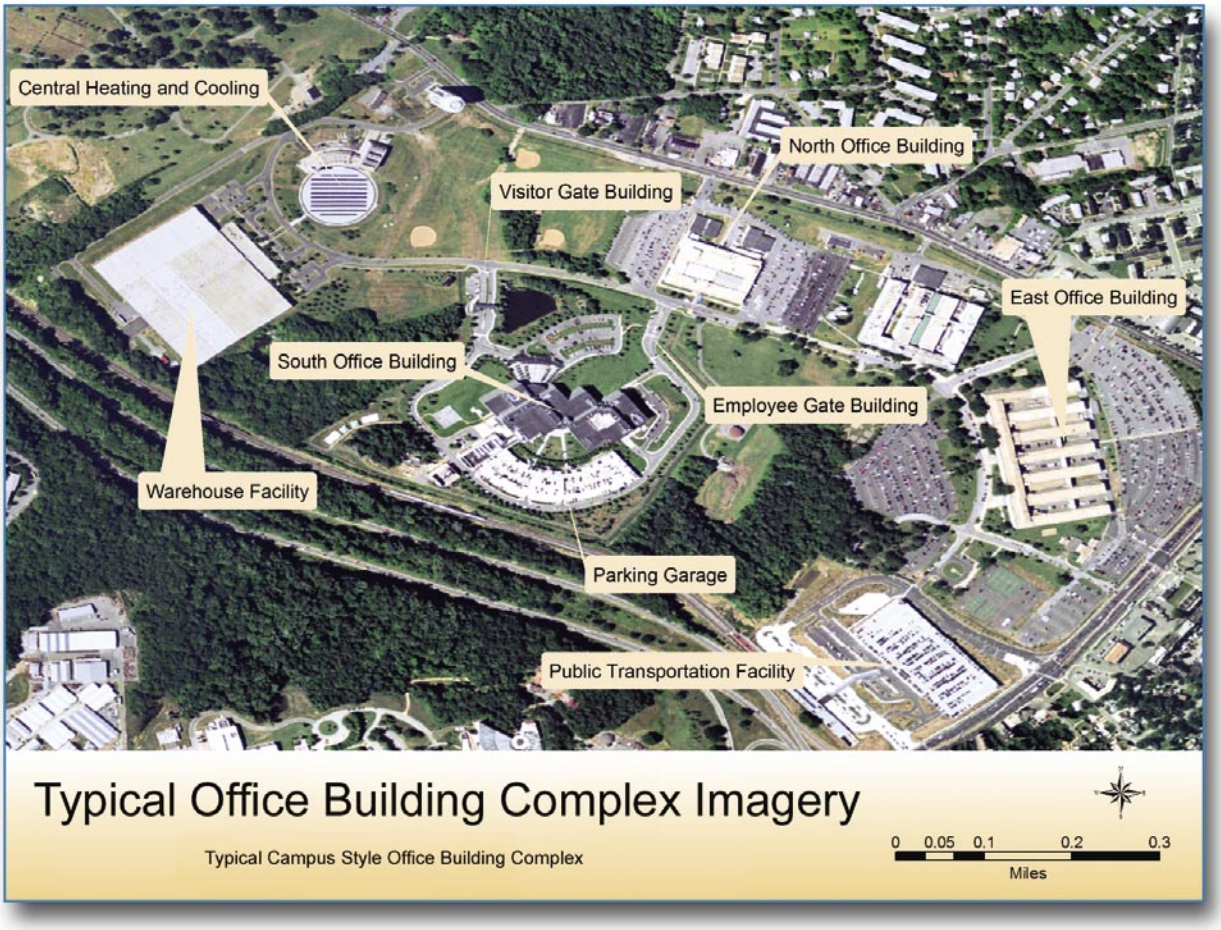


Figure 1-4 Satellite imagery/GIS tool

quantity against which to design. Second, by considering all threats/hazards (especially manmade threats) early in the design, there are potential synergies among mitigating actions. One mitigation strategy can be beneficial against more than one hazard for little difference in cost. As an example, designing moment frame connections between floors and columns and reinforcing exterior walls can mitigate against winds, explosive blasts, and earthquakes. Thus, in order to design mitigation measures for manmade hazards, the designer must have some appreciation of the assessment of threat/hazard, asset value, vulnerability, and risk to assist the building owner/decision-maker.

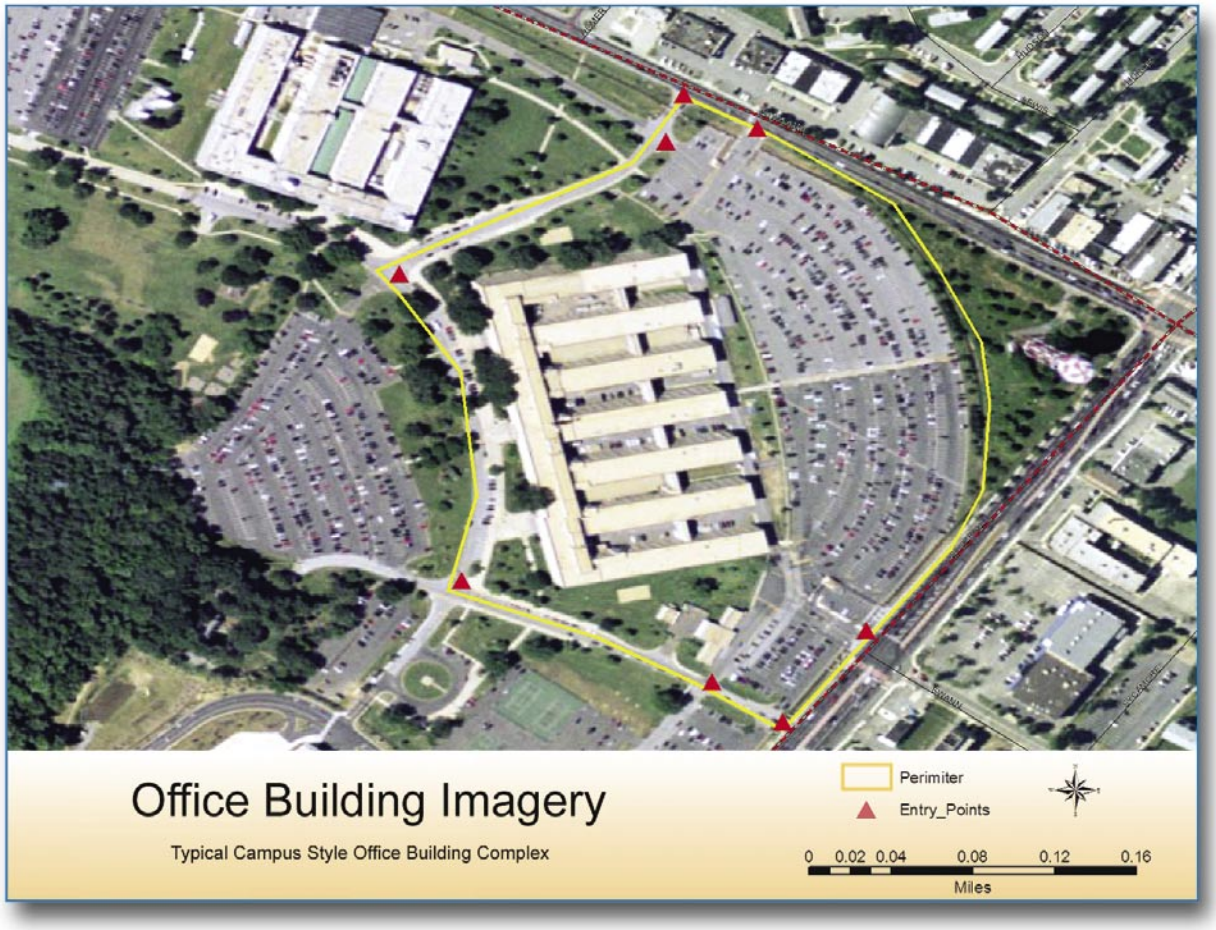


Figure 1-5 Satellite imagery/GIS tool

Based on the methodologies discussed in this chapter, the assessment process follows a logical flow:

- **Asset Value**
  - Identify criticality of assets
  - Identify number of people in a building
- **Threat/Hazard Assessment**
  - Identify each threat/hazard
  - Define each threat/hazard
  - Determine threat level for each threat/hazard
- **Vulnerability Assessment**
  - Identify site and building systems design issues

- Evaluate design issues against type and level of threat
- Determine level of protection sought for each mitigation measure against each threat

❍ **Risk Assessment**

- Likelihood of occurrence
- Impact of occurrence (loss of life, property, and function)
- Determine relative risk for each threat against each asset
- Select mitigation measures that have the greatest benefit/cost for reducing risk

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.

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. Mitigation measures may also reduce risk of damage or injury by providing an acceptable level of protection if the hazard does occur, which may also serve to further deter an aggressor. For example, the Murrah Federal Building in Oklahoma City became the target of an aggressor when he was deterred from attacking his primary target, the Federal Bureau of Investigation (FBI) building, because it was too difficult to get the attack vehicle close to the FBI building. He was able to park immediately adjacent to the Murrah Federal Building and successfully target the office of the Bureau of Alcohol, Tobacco, and Firearms (ATF), which was located in the Murrah Federal Building.

The remainder of this chapter describes the general concepts of asset value, threat/hazard, vulnerability, and risk assessments for manmade disasters and presents several methodologies and techniques that can be used by an organization in conducting these assessments.

1.1 ASSET VALUE ASSESSMENT

This section will describe how to perform an asset value assessment (the first step of the assessment process), to identify people and the asset value. To facilitate identifying people and the value of a building's assets, it is useful to conduct interviews of the people who are most familiar with them. Inputs from building owners, facility staff, and tenants, as well as any others who can help identify the most valuable assets, should be sought. In order to conduct productive interviews, a list of areas to be covered should be generated and prioritized prior to the actual interviews. Thorough planning and research to generate relevant questions will aid the process and yield better results.

An asset is a resource of value requiring protection.[1] An asset can be tangible (e.g., tenants, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company's reputation). In order to achieve the greatest risk reduction at the least cost, identifying and prioritizing a building's critical assets is a vital first step in the process to identify the best mitigation measures to improve its level of protection prior to a terrorist attack. Recognizing that people are a building's most critical asset, the process described below will help identify and prioritize infrastructure where people are most at risk and require protection.

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

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

Step 2: Identify building infrastructure

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

[1] Appendix B is a glossary of assessment and security terminology. Appendix C contains chemical, biological, and radiological terms.

1.1.1 Identifying Building Core Functions

The initial step of an asset value assessment is the determination of 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 design 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?

1.1.2 Identifying Building Infrastructure

After the core functions and processes are identified, an evaluation of building infrastructure is the next step. 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 building functions, services, or occupant satisfaction 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.
- 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 (IT - 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.

1.1.3 Quantifying Asset Value

After a list of a building's assets or resources of value requiring protection have been identified, they should be assigned a value. Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets. There are many scales that can be used, each with advantages and disadvantages. Because some people are used to working with linguistic scales, although many engineers and designers prefer numerical systems, this publication will use a combination of a seven-level linguistic scale and a ten-point numerical scale as

shown in Table 1-1. Obviously, the key asset for every building is its people (e.g., employees, visitors, etc.). They will always be assigned the highest asset value as in the example below.

Table 1-1: Asset Value Scale

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

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 – 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 – 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 – 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 – 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 – 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 – Loss or damage of the building's assets would have negligible consequences or impact.

Asset Value Example. A nominal list of assets for a typical building with assigned value is presented in Table 1-2. Please note that this is a nominal example; each building should tailor its list to its own unique situation.

Table 1-2: Nominal Building Asset Value Assessment

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

1.2 THREAT/HAZARD ASSESSMENT

1.2.1 Threat/Hazard Identification

With any manmade hazard, it is important to understand who are the people with the intent to cause harm. For those people, it is essential to understand their weapons, tools, and tactics, realizing that weapons, tools, and tactics can change faster than a building can be modified against the threat. The threat/hazard assessment information should be sought from local law enforcement, local

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

The aggressors (those people with intent to do harm) seek publicity for their cause, monetary gain (in some instances), or political gain through their actions. These actions injure or kill people; destroy or damage facilities, property, equipment, or resources; or steal equipment, material, or information. Their methods can be forced entry tools, vehicles, and surveillance (visual/audio; stand-off or planted). Their weapons can include incendiary devices; small arms (rifles and handguns); stand-off military-style weapons (rocket propelled grenades or mortars) (see Figure 1-6); explosives; and chemical, biological, and radiological agents (CBR, individually or combined with explosives to aid in dispersion).

Figure 1-6 Aggressor weapons

Explosives include homemade and stolen industrial and military varieties, packaged from small to very large (mail bombs to vehicle bombs). Aggressor tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed

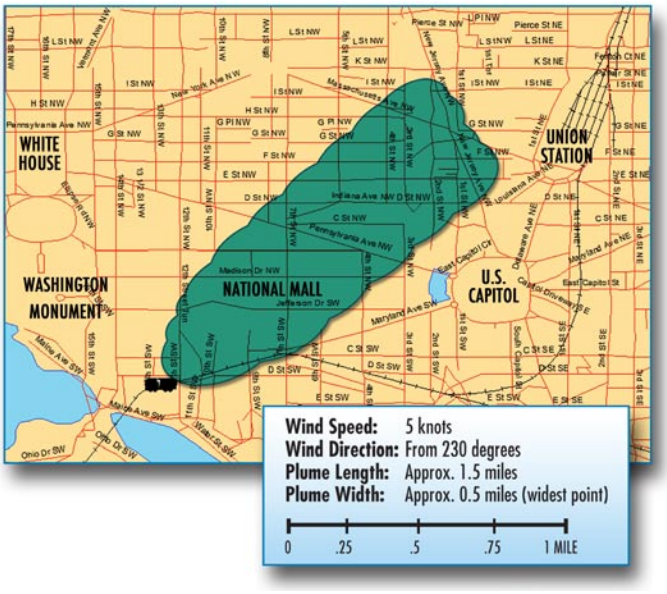


Figure 1-7 Estimated plume from a 1-ton chlorine spill in Washington, DC

bombs); stand-off weapons attacks (military or improvised larger direct and indirect fire weapons); 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 (CBR agents used to contaminate the air supply of a building as notionally (hypothetically) demonstrated in Figure 1-7); and waterborne contamination (CBR agents injected into the water supply).

Table 1-3 provides insight into the various manmade hazards to consider and can be used as a tool for threat assessments. Note that Table 1-1 combines aspects of tools, weapons, explosives, and tactics. Chapters 4 and 5 provide additional information on manmade hazards, and Appendix C provides a complete list of CBR agents.

Table 1-3 provides the designer with a general profile of events associated with a spectrum of threats/hazards. The next sections will begin the process of quantifying a building's "design basis" by applying a systems engineering evaluation process to determine a building's critical functions, infrastructure, and vulnerabilities using an understanding of the aggressors, potential threat elements, a more refined definition of the threat/hazard, and methods to evaluate the risk. There are several methodologies and assessment techniques that can be used. Historically, the U.S. military methodology (with a focus on explosive effects, CBR, and personnel protection) has been used extensively for military installations and other national infrastructure assets. The DOS adopted many of the same blast and CBR design criteria, and the GSA further developed criteria for federal buildings as a result of the

attack on the Murrah Federal Building. The Department of Commerce (DOC) Critical Infrastructure Assurance Office (CIAO) established an assessment framework, which focused on information technology infrastructure.

Table 1-3: Event Profiles for Terrorism and Technological Hazards*

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Improvised Explosive Device (Bomb) - Stationary Vehicle - Moving Vehicle - Mail - Supply - Thrown - Placed - Personnel	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/hazard 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.
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 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.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Arson/Incendiary Attack	Initiation of fire or explosion on or near target via direct contact or remotely via projectile.	Generally minutes to hours.	Extent of damage is determined by type and quantity of device /accelerant and materials present at or near target. Effects generally static other than cascading consequences, incremental structural failure, etc.	Mitigation factors include built-in fire detection and protection systems and fire-resistive construction techniques. Inadequate security can allow easy access to target, easy concealment of an incendiary device, and undetected initiation of a fire. Non-compliance with fire and building codes as well as failure to maintain existing fire protection systems can substantially increase the effectiveness of a fire weapon.
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.
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; the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Cyberterrorism	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.
Agriterrorism	Direct, generally covert contamination of food supplies or introduction of pests and/or disease agents to crops and livestock.	Days to months.	Varies by type of incident. Food contamination events may be limited to discrete distribution sites, whereas pests and diseases may spread widely. Generally no effects on built environment.	Inadequate security can facilitate adulteration of food and introduction of pests and disease agents to crops and livestock.
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.
Nuclear Device	Detonation of nuclear device underground, at the surface, in the air or at high altitude.	Light/heat flash and blast/shock wave last for seconds; nuclear radiation and fallout hazards can persist for years. Electromagnetic pulse from a high-altitude detonation lasts for seconds and affects unprotected electronic systems.	Initial light, heat, and blast effects of a subsurface, ground, or air burst are static and are determined by the device's characteristics and employment; fallout of radioactive contaminants may be dynamic, depending on meteorological conditions.	Harmful effects of radiation can be reduced by minimizing the time of exposure. Light, heat, and blast energy decrease logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc., can provide shielding by absorbing and/or deflecting blast, radiation, and radioactive contaminants.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Hazardous Material Release **(fixed site or transportation)** - Toxic Industrial Chemicals and Materials (Organic vapors: cyclohexane; Acid gases: cyanogens, chlorine, hydrogen sulfide; Base gases: ammonia; Special cases: phosgene, formaldehyde)	Solid, liquid, and/or gaseous contaminants may be released from fixed or mobile containers.	Hours to days.	Chemicals may be corrosive or otherwise damaging over time. Explosion and/or fire may be subsequent. Contamination may be carried out of the incident area by persons, vehicles, water, and wind.	As with chemical weapons, weather conditions will directly affect how the hazard develops. 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. Non-compliance with fire and building codes as well as failure to maintain existing fire protection and containment features can substantially increase the damage from a hazardous materials release.
Unauthorized Entry - Forced - Covert	Use of hand or power tools, weapons, or explosives to create a man-sized opening or operate an assembly (such as a locked door), or use of false credentials to enter a building.	Minutes to hours, depending upon the intent.	If goal is to steal or destroy physical assets or compromise information, the initial effects are quick, but damage may be long lasting. If intent is to disrupt operations or take hostages, the effects may last for a long time, especially if injury or death occurs.	Standard physical security building design should be the minimum mitigation measure. For more critical assets, additional measures, like closed circuit television or traffic flow that channels visitors past access control, aids in detection of this hazard.

Table 1-3: Event Profiles for Terrorism and Technological Hazards* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Surveillance - Acoustic - Electronic eavesdropping - Visual	Stand-off collection of visual information using cameras or high powered optics, acoustic information using directional microphones and lasers, and electronic information from computers, cell phones, and hand-held radios. Placed collection by putting a device "bug" at the point of use.	Usually months.	This is usually the prelude to the loss of an asset. A terrorist surveillance team spends much time looking for vulnerabilities and tactics that will be successful. This is the time period that provides the best assessment of threat because it indicates targeting of the building.	Building design, especially blocking lines of sight and ensuring the exterior walls and windows do not allow sound transmission or acoustic collection, can mitigate this hazard.

* SOURCE: FEMA 386-7, *INTEGRATING HUMAN-CAUSED HAZARDS INTO MITIGATION PLANNING*, SEPTEMBER 2002

1.2.2 Threat Definition of Physical Attack on a Building

To stop a terrorist or physical attack on a building is very difficult; any building or site can be breached or destroyed. 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, 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. A manmade threat/hazard analysis requires interface with security and intelligence organizations that understand the locality, the region, and the nation. These organizations include the police department (whose jurisdiction includes the building or site), the local state police office, and the local office of the FBI. In many areas of the country, there are threat coordinating committees, including FBI Joint Terrorism Task Forces, that facilitate the sharing of informa-

tion. A common method to evaluate terrorist threats is to analyze five factors: existence, capability, history, intention, and targeting.

Existence addresses the questions: Who is hostile to the assets, organization, or community of concern? Are they present or thought to be present? Are they able to enter the country or are they readily identifiable in a local community upon arrival?

Capability addresses the questions: What weapons have been used in carrying out past attacks? Do the aggressors need to bring them into the area or are they available locally?

History addresses the questions: What has the potential threat element done in the past and how many times? When was the most recent incident and where, and against what target? What tactics did they use? Are they supported by another group or individuals? How did they acquire their demonstrated capability?

Intention addresses the questions: What does the potential threat element or aggressor hope to achieve? How do we know this (e.g., published in books or news accounts, speeches, letters to the editor, informant)?

Targeting addresses the questions: Do we know if an aggressor (we may not know which specific one) is performing surveillance on our building, nearby buildings, or buildings that have much in common with our organization? Is this information current and credible, and indicative of preparations for terrorist operations (manmade hazards)?

The threat/hazard analysis for any building can range from a general threat/hazard 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.

A terrorist or aggressor will analyze the building or target as shown in Figure 1-8 to determine the type of attack, type of weapon, and tactics to employ to defeat the building or critical mission/ business function.

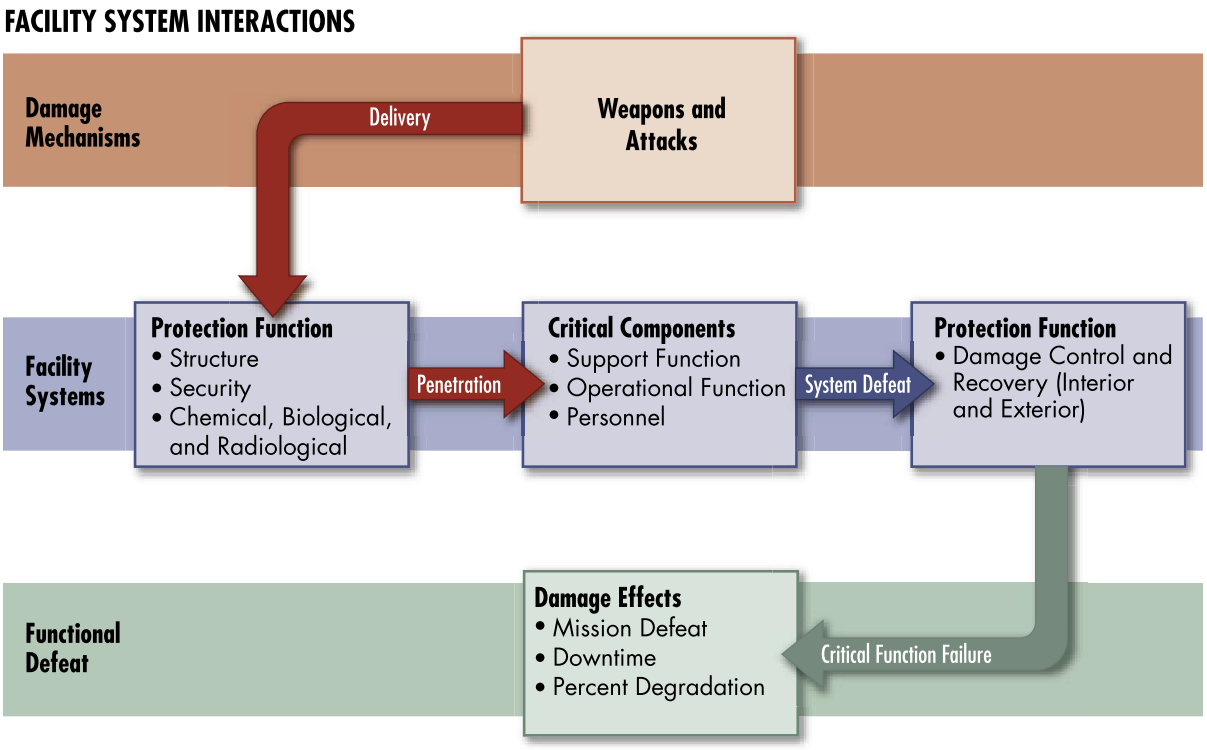


Figure 1-8 Facility system interactions

The Homeland Security Advisory System has five threat levels that provide a general indication of risk of terrorist attack. In Table 1-4, the five factors commonly used to evaluate terrorist threats have been layered onto the Homeland Security Advisory levels. If the anticipated threat or projected use of the building warrants it, a detailed threat analysis should be developed in coordination with local law enforcement, intelligence, and civil authorities in order to more quantitatively determine the vulnerability or risk. Having conducted a threat analysis and having a good conceptual idea of the preliminary building design and site layout, the next step is to conduct a vulnerability assessment to identify weaknesses that can be exploited by an aggressor and to help identify specific design features and establish operational parameters to mitigate them.

Table 1-4: Homeland Security Threat Conditions

Threat Level	Threat Analysis Factors				
	Existence	Capability	History	Intentions	Targeting
Severe (Red)	●	●	●	●	●
High (Orange)	●	●	●	●	❑
Elevated (Yellow)	●	●	●	❑	
Guarded (Blue)	●	●	❑		
Low (Green)	●	❑			

● Factor must be present ❑ Factor may or may not be present

Please note the DHS does not use these threat analysis factors to determine threat level.

SOURCE: COMMONWEALTH OF KENTUCKY OFFICE OF HOMELAND SECURITY

1.3 VULNERABILITY ASSESSMENT

Knowing the expected threat/hazard capability allows the designer to integrate the threat knowledge with specific building and site information by conducting a vulnerability assessment. A vulnerability assessment is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities. A vulnerability assessment should be performed for existing buildings and the process incorporated into the design for new construction and renovation.

Table 1-5 contains vulnerability and consequence aspects and provides an objective approach to determine a relative value of vulnerability for the building or site. An alternate method for determining a relative value is presented in Table 1-6, from the U.S. Department of Justice (DOJ), as applicable to GSA buildings. This method provides a suggestion of "security measures" for typical sizes and types of sites, in addition to a transferable example of appropriate security measures for typical locations and occupancies. Tables 1-5 and 1-6 address operational, consequential, and inherent characteristics that contribute to vul-

nerability. They are a first step and should be used in conjunction with a more detailed vulnerability assessment such as the Building Vulnerability Assessment Checklist (see Table 1-22).

Table 1-7 is an example of one approach to implement minimum building design standards to mitigate terrorist events following the methodology of Table 1-6. Note that an evaluation or vulnerability assessment still needs to be done before incorporating any mitigation measures.

Table 1-5: Site/Building Inherent Vulnerability Assessment Matrix (Partial Risk Assessment)*

Criteria	0	1	2	3	4	5	Score
Asset Visibility	—	Existence not well known	—	Existence locally known	—	Existence widely known	
Target Utility	None	Very Low	Low	Medium	High	Very High	
Asset Accessibility	Remote location, secure perimeter, armed guards, tightly controlled access	Fenced, guarded, controlled access	Controlled access, protected entry	Controlled access, unprotected entry	Open access, restricted parking	Open access, unrestricted parking	
Asset Mobility	—	Moves or is relocated frequently	—	Moves or is relocated occasionally	—	Permanent/ fixed in place	
Presence of Hazardous Materials	No hazardous materials present	Limited quantities, materials in secure location	Moderate quantities, strict control features	Large quantities, some control features	Large quantities, minimal control features	Large quantities, accessible to non-staff personnel	
Collateral Damage Potential	No risk	Low risk/ limited to immediate area	Moderate risk/limited to immediate area	Moderate risk within 1-mile radius	High risk within 1-mile radius	High risk beyond 1-mile radius	
Site Population/ Capacity	0	1-250	251-500	501-1,000	1,001-5,000	> 5,000	
						Total	

* SOURCE: FEMA 386-7, *INTEGRATING HUMAN-CAUSED HAZARDS INTO MITIGATION PLANNING*, SEPTEMBER 2002

Table 1-6: Classification Table Extracts*

Level**	Typical Location	Examples of Tenant Agencies***	Security Measures (based on evaluation)
I	10 Employees (Federal) 2,500 Square Feet Low Volume Public Contact Small "Store Front" Type Operation	Local Office District Office Visitor Center USDA Office Ranger Station Commercial Facilities Industrial/Manufacturing Health Care	High Security Locks Intercom Peep Hole (Wide View) Lighting w/Emergency Backup Power Controlled Utility Access Annual Employee Security Training
II	11 - 150 Employees (Federal) 2,500 - 80,000 Square Feet Moderate Volume Public Contact Routine Operations Similar to Private Sector and/or Facility Shared with Private Sector	Public Officials Park Headquarters Regional/State Offices Commercial Facilities Industrial Manufacturing Health Care	Entry Control Package w/Closed Circuit Television (CCTV) Visitor Control/Screening Shipping/Receiving Procedures Guard/Patrol Assessment Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt, Zoom System) Duress Alarm w/Central Monitoring
III	151 - 450 Employees (Federal) Multi-Story Facility 80,000 - 150,000 Square Feet Moderate/High Volume Public Contact Agency Mix: Law Enforcement Operations Court Functions Government Records	Inspectors General Criminal Investigations Regional/State Offices GSA Field Office Local Schools Commercial Facilities Industrial Manufacturing Health Care	Guard Patrol on Site Visitor Control/Screening Shipping/Receiving Procedures Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt/Zoom System) Duress Alarm w/Central Monitoring
IV	>450 Employees (Federal) Multi-Story Facility >150,000 Square Feet High Volume Public Contact High-Risk Law Enforcement/Intelligence Agencies District Court	Significant Buildings and Some Headquarters Federal Law Enforcement Agencies Local Schools, Universities Commercial Facilities Health Care	Extend Perimeter (Concrete/Steel Barriers) 24-Hour Guard Patrol Adjacent Parking Control Backup Power System Hardened Parking Barriers
V	Level IV Profile and Agency/Mission Critical to National Security	Principal Department Headquarters	Agency-Specific

* 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

Table 1-7: Selected Extracts -- Recommended Standards Chart*

M – Minimum Standard
D – Desirable (to minimize risk)
S – Standard Based On Facility Evaluation
N/A – Not Applicable

	LEVEL				
	I	II	III	IV	V
PERIMETER SECURITY					
Parking					
Control of Facility Parking	D	D	M	M	M
Control of Adjacent Parking	D	D	D	S	S
Avoid Leases Where Parking Cannot be Controlled	D	D	D	D	D
Leases Should Provide Security Control for Adjacent Parking	D	D	D	D	D
Post Signs and Arrange for Towing Unauthorized Vehicles	S	S	M	M	M
ID System and Procedures for Authorized Parking (Placard, Decal, Card Key, etc.)	D	D	M	M	M
Adequate Lighting for Parking Areas	D	D	M	M	M
Closed Circuit Television (CCTV) Monitoring					
CCTV Surveillance Cameras with Time Lapse Video Recording	D	S	S	M	M
Post Signs Advising of 24-Hour Video Surveillance	D	S	S	M	M
Lighting					
Lighting with Emergency Power Backup	M	M	M	M	M
Physical Barriers					
Extend Physical Perimeter with Barriers (Concrete and/or Steel Composition)	N/A	N/A	D	S	S
Parking Barriers	N/A	N/A	D	S	S
ENTRY SECURITY					
Receiving/Shipping					
Review Receiving/Shipping Procedures (Current)	M	M	M	M	M
Implement Receiving/Shipping Procedures (Modified)	D	S	M	M	M
Access Control					
Evaluate Facility for Security Guard Requirements	D	S	M	M	M
Security Guard Patrol	D	D	S	S	S
Intrusion Detection System with Central Monitoring Capability	D	S	M	M	M
Upgrade to Current Life Safety Standards (Fire Detection, Fire Suppression Systems, etc.)	M	M	M	M	M
Entrances/Exits					
X-Ray and Magnetometer at Public Entrances	N/A	D	S	S	M
Require X-Ray Screening of All Mail/Packages	N/A	D	S	M	M
Peep Holes	S	S	N/A	N/A	N/A
Intercom	S	S	N/A	N/A	N/A
Entry Control w/CCTV and Door Strikes	D	S	N/A	N/A	N/A
High Security Locks	M	M	M	M	M

Table 1-7: Selected Extracts -- Recommended Standards Chart* (continued)

M – Minimum Standard
D – Desirable (to minimize risk)
S – Standard Based On Facility Evaluation
N/A – Not Applicable

	LEVEL				
	I	II	III	IV	V
INTERIOR SECURITY					
Employee/Visitor Identification					
Agency Photo ID for all Personnel Displayed at all Times	N/A	D	S	M	M
Visitor Control/Screening System	D	M	M	M	M
Visitor Identification Accountability System	N/A	D	S	M	M
Establish ID Issuing Authority	S	S	S	M	M
Utilities					
Prevent Unauthorized Access to Utility Areas	S	S	M	M	M
Provide Emergency Power to Critical Systems (Alarm Systems, Radio Communications, Computer Facilities, etc.)	M	M	M	M	M
Daycare Centers					
Evaluate Whether to Locate Daycare Facilities in Buildings with High-Threat Activities	N/A	M	M	M	M
Compare Feasibility of Locating Daycare in Facilities Outside Locations	N/A	M	M	M	M
SECURITY PLANNING					
Tenant Assignment					
Collocate Agencies with Similar Security Needs	D	D	D	D	D
Do Not Collocate High-/Low-Risk Agencies	D	D	D	D	D
Administrative Procedures					
Arrange for Employee Parking In/Near Building After Normal Work Hours	S	S	S	S	S
Conduct Background Security Checks and/or Establish Security Control Procedures for Service Contract Personnel	M	M	M	M	M
Construction/Renovation					
Install Mylar Film on all Exterior Windows (Shatter Protection)	D	D	S	M	M
Review Current Projects for Blast Standards	M	M	M	M	M
Review/Establish Uniform Standards for Construction	M	M	M	M	M
Review/Establish New Design Standard for Blast Resistance	S	S	M	M	M
Establish Street Setback for New Construction	D	D	S	M	M

* SOURCE: EXTRACTS FROM U.S. DEPARTMENT OF JUSTICE STUDY "*VULNERABILITY ASSESSMENT OF FEDERAL FACILITIES*," JUNE 28, 1995

In the preceding tables, determining which "level" most nearly reflects the site and building under design or renovation may help to identify which security standards would be most appropriate to apply. The GSA method provides a more detailed analysis of a building vulnerability and good suggestions for security measures that may be appropriate to design into a building for certain occupancies and sizes of facilities. A more quantitative evaluation or ranking of one building compared to another may be required in some instances (e.g., where a building owner and designer may need to know the relative risk of one building compared to an equivalent building on another site or on the same campus).

The DOJ, Office of Justice Programs (OJP) provides an objective approach to determining vulnerability (see U.S. Department of Justice, Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit, May 15, 1999). DOJ's Threat/Hazard Assessment uses seven factors that are Threat Assessment and Consequence Management oriented, and provides a quantitative means to rank buildings. It requires rating each of the seven areas and summing the ratings to determine the overall ranking for the building or site. This approach is as follows:

1. Level of Visibility (Table 1-8)
What is the perceived awareness of the target's existence and the visibility of the target to the general populace, or to the terrorist in particular?

Table 1-8: Level of Visibility

	Rating Value
Invisible – Classified location	0
Very Low Visibility – Probably not aware of existence	1
Low Visibility – Existence probably not well known	2
Medium Visibility – Existence is probably known	3
High Visibility – Existence is well known	4
Very High Visibility – Existence is obvious	5

2. Asset Value of Target Site (Individual Asset or Assets Accumulated within Building – Table 1-9)

What is the usefulness of the asset(s) to the population, economy, government, company, or organization? Also consider the impact on continuity of operations, hampering of emergency response, and general potential consequences. Table 1-9 could be used more than once if the value of the asset(s) impacts more than one critical area.

Table 1-9: Criticality of Target Site

	Rating Value
No Usefulness	0
Minor Usefulness	1
Moderate Usefulness	2
Significant Usefulness	3
Highly Useful	4
Critical	5

3. Target Value to Potential Threat Element/Aggressor (Table 1-10)

Does the target serve the ends of the aggressors identified in the Threat Assessment based on motivations (political, religious, racial, environmental, and special interests)? Table 1-10 should help to capture these motivations.

Table 1-10: Target Value to Potential Threat Element

	Rating Value
None	0
Very Low	1
Low	2
Medium	3
High	4
Very High	5

4. Aggressor Access to Target (Table 1-11)

Does the target have available ingress and egress for a potential aggressor?

Table 1-11: Aggressor Access to Target

	Rating Value
Fenced, Guarded, Protected Air/Consumable Entry, Controlled Access by Pass Only, No Vehicle Parking within a designated minimum distance (such as 50 feet or 80 feet)	0
Guarded, Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel, No Vehicle Parking within the designated minimum distance	1
Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel, No Unauthorized Vehicle Parking within the designated minimum distance	2
Controlled Access of Visitors, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within the designated minimum distance	3
Open Access to All Personnel, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within the designated minimum distance	4
Open Access to All Personnel, Unprotected Air/Consumable Entry, Vehicle Parking within the designated minimum distance	5

5. Target Threat of Hazard (Table 1-12)

Are CBR materials present in quantities that could become hazardous if released? These quantities could be on site or in relatively close proximity so that a theft or an accident could render them a hazard to the building or site. Take into consideration distance from building (a 1-mile radius is suggested around the building), the prevailing wind direction, the slope of the terrain, and the quantity of materials present.

Table 1-12: Target Threat of Hazard (WMD Materials)

	Rating Value
No CBR materials present	0
CBR materials present in moderate quantities, under positive control, and in secured locations	1
CBR materials present in moderate quantities and controlled	2
Major concentrations of CBR materials that have established control features and are secured in the site	3
Major concentrations of CBR materials that have moderate control features	4
Major concentrations of CBR materials that are accessible to non-staff personnel	5

6. Site Population Capacity (Table 1-13)
What is the maximum number of individuals at the building or site at a given time? This could be standard worst case occupancy during an average day or peak occupancy at a designated time (e.g., a movie theater).

Table 1-13: Site Population Capacity

	Rating Value
0	0
1 to 250	1
251 to 500	2
501 to 1,000	3
1,001 to 5,000	4
> 5,000	5

7. Potential for Collateral Damage (Mass Casualties - Table 1-14)
Address potential collateral mass casualties within a 1-mile radius of the target site. Number ranges indicate inhabitants within a 1-mile radius of the site.

Table 1-14: Potential for Collateral Damage (Mass Casualties)

	Rating Value
0-100	0
101 to 500	1
501 to 1,000	2
1,001 to 2,000	3
2,001 to 5,000	4
> 5,000	5

Each building is assessed and scored (see Table 1-15). Tables 1-15 and 1-16 contain a nominal example.

Table 1-15: Building Summary Sheet

Building/Target Name	Score
Visibility	4
Criticality	3
Value	4
Access	2
Threat of Hazard	0
Site Population	3
Collateral Mass Casualties	3
Total Score	19

The total building score can be used to rank multiple buildings (see Table 1-16) and quantitatively provides an analysis of building vulnerability from a site perspective.

Table 1-16: Building Ranking

Ranking	Building/Target Name	Total Score
1	ABC Building	23
2	DEF Building	19
3	GHI Building	14

This evaluation methodology can be applied to all building types (see Foreword). The result is independent of facility/occupancy type, except for the type of influence on population and siting.

An alternate approach is shown in Table 1-17, which uses a simplified matrix to rank the order of buildings using a numerical score of 1 (low) to 5 (high). The evaluation factors can be developed for each building use or owner-specific criteria. For Table 1-17, the factors shown illustrate a health care provider scenario:

- Criticality of Function: How critical is the building and function to the organization?

- Location: Is the building near federal buildings, major transportation, or iconic properties?
- Occupancy of Building: Are occupants mobile or non-ambulatory?
- Involvement in Community: Does the building or staff provide unique capabilities?
- Critical External Commitments: Does the building support other organizations or missions?

Table 1-17: Simplified Building Ranking Matrix

Building	Criticality of Function	Location	Occupancy of Building	Involvement in Community	Critical External Commitments	Total Score
Headquarters	2	5	3	1	4	15
Hospital 1	1	2	2	1	1	7
Hospital 2	3	2	3	4	4	16
Data Center	5	4	3	3	2	17

The objective of Tables 1-1 through 1-17 or similar assessment methodologies is to provide an analysis of a building, facility, or site and to identify the buildings that are most vulnerable from a given threat/hazard matched against specific building type or function. Having the ranked list of buildings, the next step is to conduct an in-depth vulnerability assessment of the building. The building assessment is to evaluate specific design and architectural features and identify all vulnerabilities of the building functions and building systems. Frequently, single-point-vulnerabilities exist, which are critical functions or systems that lack redundancy and, if damaged by an attack, would result in immediate organization disruption or loss of capability. These are generally the highest risk vulnerabilities. Figure 1-9 illustrates the common system vulnerabilities.

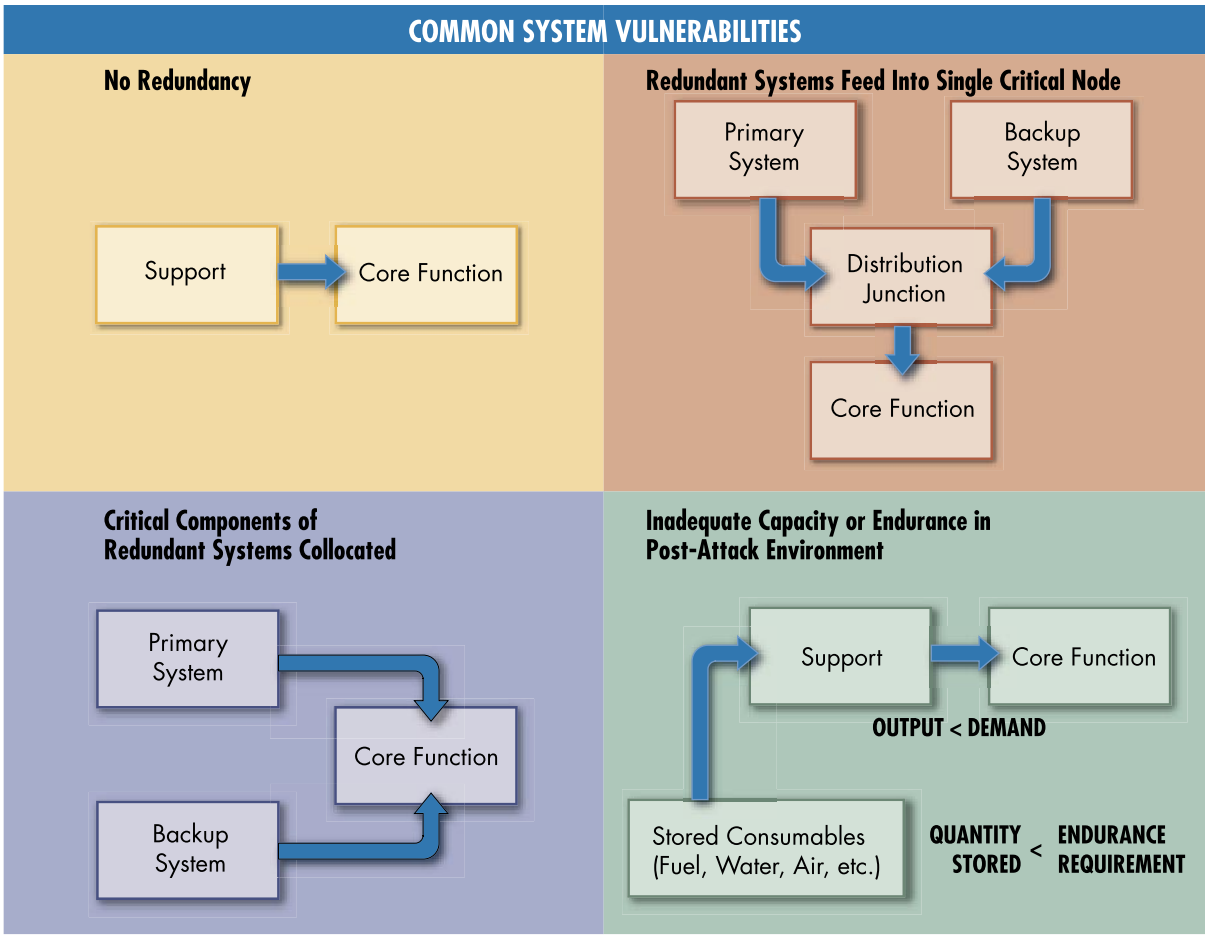


Figure 1-9 Common system vulnerabilities

1.4 RISK ASSESSMENT

Risk is the potential for a loss of 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), and asset value and vulnerabilities (consequences of the occurrence) 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. Chapters 2 and 3 explore mitigation measures to reduce the vulnerability and risk for valuable assets with a high risk.

There are numerous methodologies and technologies for conducting a risk assessment. One approach is to assemble the results of the asset value assessment, threat 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

This methodology can be used for new buildings during the design process, as well as for existing structures. The first task is to identify the value of assets and people that need to be protected. Next, a threat assessment is performed to identify and define the threats and hazards that could cause harm to a building and its inhabitants. After threats and assets are identified, a vulnerability assessment is performed to identify weaknesses that might be exploited by a terrorist or aggressor. Using the results of the asset value, threat, and vulnerability assessments, risk can be computed.

After the architect and building engineer know how people and assets are at greatest risk against specific threats, they can then identify mitigation measures to reduce risk. Because it is not possible to completely eliminate risk, and every project has resource limitations, architects and engineers must analyze how mitigation measures would affect risk and decide on the best and most cost-effective measures to implement to achieve the desired level of protection (risk management).

There are numerous checklists and techniques to use for conducting an individual building risk assessment. A simplified approach is presented in Tables 1-18 through 1-21. The tables are used as a pre-assessment screening tool by the assessor who conducts an interview with several key staff members (e.g., building owner, security, site management, key function representatives, etc.). The interview provides a consensus judgment of the relative risk or vulnerability of functions or systems and should also identify system interdependencies. Table 1-19 provides both a quantitative score and color code to objectively and visually determine the functions and systems that have been determined to

be at risk. Engineers, architects, or experienced assessors could perform a short walk-through and conduct the pre-assessment interview of an existing building in less than a day. For a new building, the pre-screening results can be used by the designer to focus the design team on incorporating features and redundancies to reduce vulnerabilities and risk.

In the risk assessment approach presented in Tables 1-18 through 1-21, three factors or elements of risk are considered for each function or system against each threat previously identified. The first factor is the value of the asset or degree of debilitating impact that would be caused by the incapacity or destruction of the asset. A value on a scale of 1 to 10 is assigned (as shown in Table 1-18), 1 being a very low impact or consequence and 10 being very high or an exceptionally grave consequence. The next factor is the threat rating or subjective judgment of a terrorist threat based on existence, capability, history, intentions, and targeting. Again, on a scale of 1 to 10, 1 is a very low probability and 10 is a very high probability of a terrorist attack. The third factor of risk is vulnerability, or any weaknesses that can be exploited by an aggressor. A value of 1 to 10 is assigned, 1 being very low or no weaknesses exist, and 10 being very high vulnerability, meaning one or more major weaknesses make an asset extremely susceptible to an aggressor. 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 in accordance with Table 1-19. 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.

Table 1-18: Risk Factors Definitions

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

Table 1-19: Total Risk Color Code

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

Table 1-20: Site Functional Pre-Assessment Screening Matrix*

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
Administration	280	140	135	90
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	7	7	9	9
Engineering	128	128	192	144
Asset Value	8	8	8	8
Threat Rating	8	4	3	2
Vulnerability Rating	2	4	8	9
Warehousing	96	36	81	54
Asset Value	3	3	3	3
Threat Rating	8	4	3	2
Vulnerability Rating	4	3	9	9
Data Center	360	128	216	144
Asset Value	8	8	8	8
Threat Rating	9	4	3	2
Vulnerability Rating	5	4	9	9

Table 1-20: Site Functional Pre-Assessment Screening Matrix* (continued)

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
Food Service	2	32	48	36
Asset Value	2	2	2	2
Threat Rating	1	4	3	2
Vulnerability Rating	1	4	8	9
Security	280	140	168	126
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	5	5	8	9
Housekeeping	16	64	48	36
Asset Value	2	2	2	2
Threat Rating	8	4	3	2
Vulnerability Rating	1	8	8	9
Day Care	54	324	243	162
Asset Value	9	9	9	9
Threat Rating	3	4	3	2
Vulnerability Rating	2	9	9	9

* NOTIONAL DATA INSERTED FOR DEMONSTRATION PURPOSES.

Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix*

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
Site	48	80	108	72
Asset Value	4	4	4	4
Threat Rating	4	4	3	2
Vulnerability Rating	3	5	9	9
Architectural	40	40	135	20
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	1	2	9	2
Structural Systems	24	32	240	16
Asset Value	8	8	8	8
Threat Rating	3	4	3	2
Vulnerability Rating	1	1	10	1
Envelope Systems	84	112	189	112
Asset Value	7	7	7	7
Threat Rating	6	4	3	2
Vulnerability Rating	2	4	9	8

Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix* (continued)

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
Utility Systems	112	56	168	42
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	2	2	8	3
Mechanical Systems	42	56	105	126
Asset Value	7	7	7	7
Threat Rating	6	4	3	2
Vulnerability Rating	1	2	5	9
Plumbing and Gas Systems	40	40	120	70
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	1	2	8	7
Electrical Systems	42	84	189	28
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	1	3	9	2
Fire Alarm Systems	162	108	216	36
Asset Value	9	9	9	9
Threat Rating	6	4	3	2
Vulnerability Rating	3	3	8	2
IT/Communications Systems	512	64	192	32
Asset Value	8	8	8	8
Threat Rating	8	4	3	2
Vulnerability Rating	8	2	8	2

* NOTIONAL DATA INSERTED FOR DEMONSTRATION PURPOSES.

The functions and infrastructure 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 pre-determined recovery site or alternate work location. Similarly, critical infrastructure should have geographic dispersion and backup. Figure 1-10 shows an example of a building that has numerous critical functions and infrastructure collocated, which creates a single-point vulnerability as illustrated below. A bomb or CBR attack entering through the loading dock could impact the telecommunications, data, uninterrupted power supply (UPS), generator, and other key infrastructure systems.

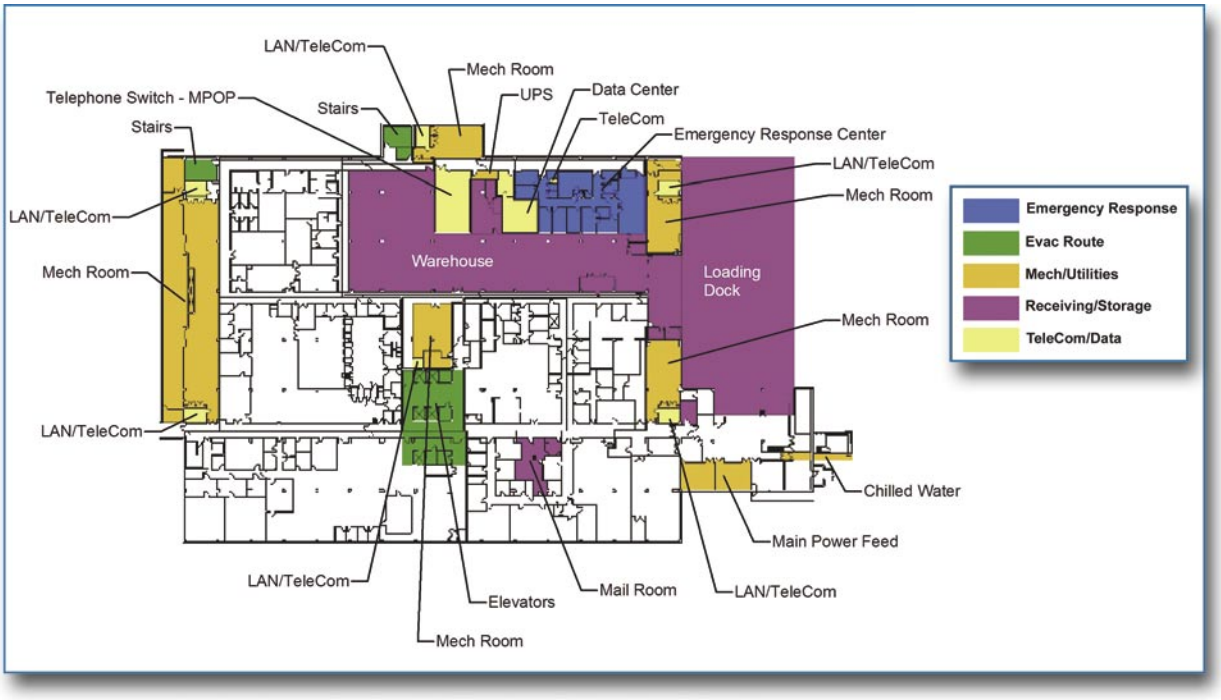


Figure 1-10 Non-redundant critical functions collocated near loading dock

As a minimum, those critical assets assessed to be at highest risk should receive an on-site vulnerability assessment using the Building Vulnerability Assessment Checklist in Table 1-22. The vulnerability assessment may change the risk rating of assets due to the identification of accessible critical nodes, the ease of attack using a common tactic, or some other factor that makes the building more attractive as a target or more susceptible to damage that could result in casualties or irrecoverable system damage. The photographs in Figure 1-11 illustrate some examples of single-point vulnerabilities of systems and infrastructure.

Figure 1-11 Vulnerability examples

1.5 RISK MANAGEMENT

Traditionally, the building regulatory system has addressed natural disaster mitigation (hurricane, tornado, flood, earthquake, windstorm, and snow storm) through prescriptive building codes supported by well-established and accepted reference standards, regulations, inspection, and assessment techniques. Some manmade risks (e.g., HazMat storage) and specific societal goals (energy conservation and life safety) have also been similarly addressed. However, the building regulation system has not yet fully addressed most manmade hazards or terrorist threats.

Soon after September 11, 2001, the New York City Building Department initiated an effort to analyze the building code with regard to terrorist threats. The task force issued a report recommending code changes based on the attack on the World Trade Center. The National Fire Protection Association (NFPA) has a committee on premises security and security system installation standards. These advances may some day result in the building regulatory system developing more prescriptive building codes to mitigate security threats.

In the absence of such regulations, the designer needs to understand on what threat the design is based. Just like seismic design requires an understanding of geology, soil structure, and the maximum credible earthquake accelerations possible at a given location, the site designer needs to comprehend the bomb size, vehicle size, and gun or other weapon size to provide an appropriate level of protection. The size of threat and desired level of protection are equally important to the design. For most cases across the United States, the threats and risks for a specific building will be low. For buildings at a higher threat and risk, higher standards and performance may be required. The Department of Defense (DoD), GSA, and DOS all have established processes to identify design basis threats for their facilities.

The typical building design and construction process is sequential, progressing from identifying building use and design goals through actual construction. This process is illustrated in Figure 1-12.

Figure 1-12 Typical building design and construction process

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

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

Figure 1-13 is a graphical representation of the three choices. Since September 11, 2001, terrorism has become a dominant concern. Life, safety, and security issues should be a design goal from the beginning.

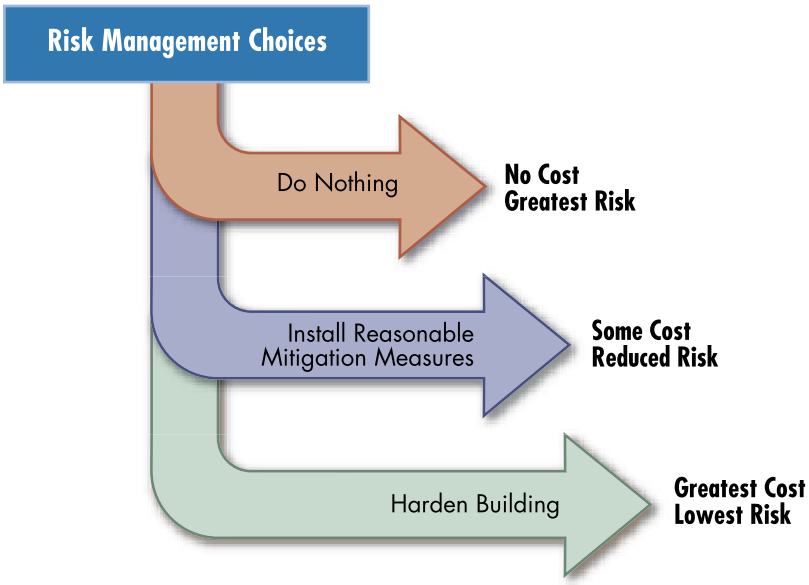


Figure 1-13 Risk management choices

Table 1-22 contains key questions that designers may use to determine vulnerabilities of an existing building or a new construction in order to focus resources and minimize the impacts of potential terrorist attacks or technological accidents.

1.6 BUILDING VULNERABILTY ASSESSMENT CHECKLIST

The Building Vulnerability Assessment Checklist (Table 1-22) is based on the checklist developed by the Department of Veterans Affairs (VA) and 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 can be used as a screening tool for preliminary design vulnerability assessment. In addition to examining design issues that affect vulnerability, the checklist includes questions that determine if critical systems continue to function in order to enhance deterrence, detection, denial, and damage limitation, and to ensure that emergency systems function during a threat or hazard situation.

The checklist is organized into the 13 sections listed below. 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.

1. Site
2. Architectural
3. Structural Systems
4. Building Envelope
5. Utility Systems
6. Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)
7. Plumbing and Gas Systems
8. Electrical Systems
9. Fire Alarm Systems
10. Communications and Information Technology (IT) Systems
11. Equipment Operations and Maintenance
12. Security Systems
13. Security Master Plan

Table 1-22: Building Vulnerablilty Assessment Checklist*

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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
		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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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. Reference: *GSA PBS-P100*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
1.19	**Do site landscaping and street furniture provide hiding places?**	Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages. If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages. Reference: *GSA PBS-P100*	
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
2.19	**Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/ alarm systems, fire suppression water mains, cooling and heating mains, etc.?**	Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against explosive blast. Consider a 50-foot separation distance in all directions. Reference: *GSA PBS-P100*	
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
2.24	**Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?**	Egress pathways should be hardened and discharge into safe areas. Reference: *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.	
2.27	**Is interior glazing near high-risk areas minimized?** **Is interior glazing in other areas shatter-resistant?**	Reference: *FEMA 386-7* 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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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**	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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	the building perimeter without progressive collapse? **In the event of an internal explosion in an uncontrolled public ground floor area, does the design prevent progressive collapse due to the loss of one primary column?** **Do architectural or structural features provide a minimum 6-inch stand-off to the internal columns (primary vertical load carrying members)?** **Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?**	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*	
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.	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
		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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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.	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	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?**	In-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures. 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?**	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.	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	How many gallons of storage capacity are available and how long will it allow operations to continue?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities.*	
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	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 pprovisions 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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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.	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
		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*	
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
		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*	
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?**	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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	Who are the manufacturers of the CCTV cameras? **What is the age of the CCTV cameras in use?**	should be considered for areas that lack adequate illumination for color cameras. Reference: *GSA PBS P-100*	
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
	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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
		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*	
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

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*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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: *DOC CIAO Vulnerability Assessment Framework 1.1*	

Table 1-22: Building Vulnerablilty Assessment Checklist* (continued)

Section	Vulnerability Question	Guidance	Observations
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