STEP 2: ASSET VALUE ASSESSMENT

OVERVIEW

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

The asset value assessment process involves the following tasks:

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

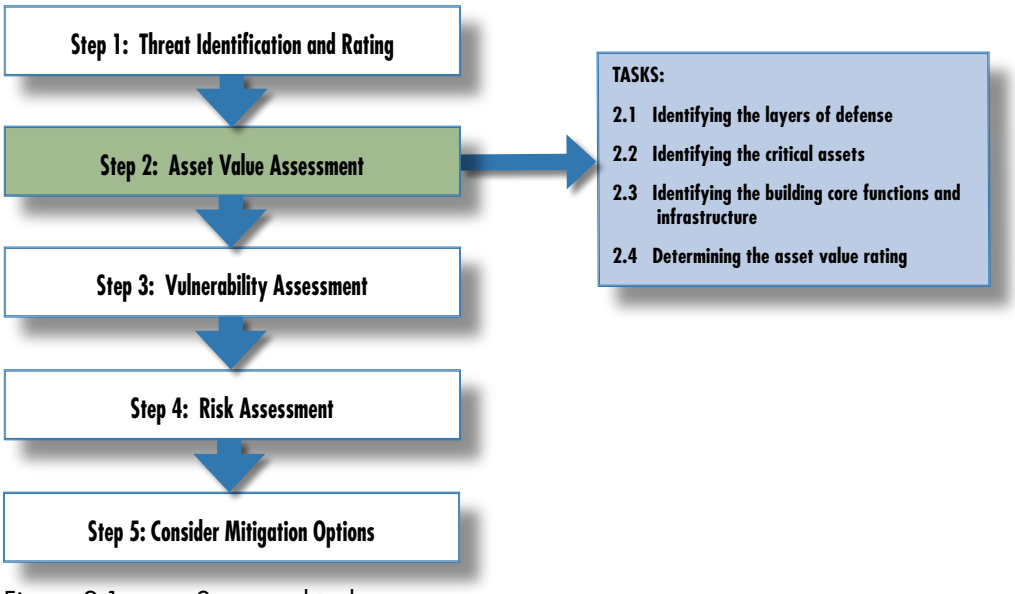


Figure 2-1 Steps and tasks

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

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

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

Identifying the Layers of Defense (Task 2.1)

The layers of defense is a traditional approach in security engineering and use concentric circles extending out from an area or site to the building or asset that requires protection. They can be seen as demarcation points for different security strategies. Identifying the layers of defense early in the assessment process will help you to understand better the assets that require protection and determine your mitigation options. Figure 2-2 shows the layers of defense described below.

First Layer of Defense. This involves understanding the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of adjacent activities. It is specifically concerned with buildings, installations, and infrastructure outside the site perimeter. For urban areas, it also includes the curb lane and surrounding streets.

Second Layer of Defense. This refers to the space that exists between the site perimeter and the assets requiring protection. It involves the placement of buildings and forms in a particular site and understanding which natural or physical resources can provide protection. It entails the design of access points, parking, roadways, pedestrian walkways, natural barriers, security lighting, and signage. For urban areas, it refers specifically to the building yard.

Third Layer of Defense. This deals with the protection of the asset itself. It proposes to harden the structures and systems, incorporate effective HVAC systems and surveillance equipment, and wisely design and locate utilities and mechanical systems. Note that, of all blast mitigation measures, distance is the most effective measure because other measures vary in effectiveness and can be more costly. However, often it is not possible to provide adequate stand-off distance. For example, sidewalks in many urban areas may be less than 10 meters (33 feet), while appropriate stand-off may require a minimum of 25 meters (82 feet).

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

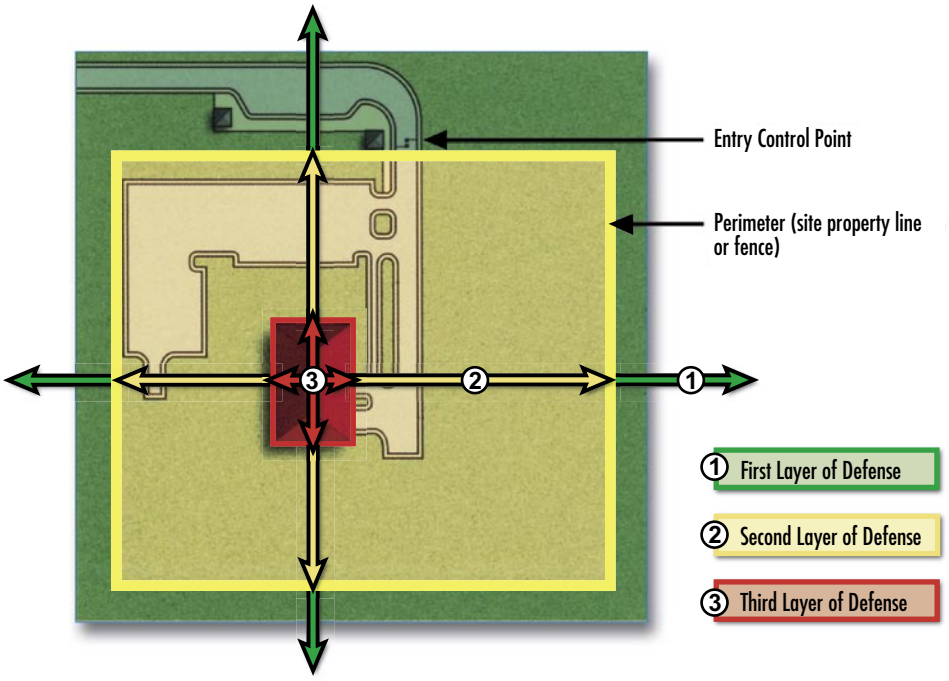


Figure 2-2 Layers of defense

Urban versus Rural

The layers of defense are not predetermined and they may vary from site to site and from building to building. If a particular building requiring protection is part of a campus or located in a rural, semi-rural, or urban area, a similar analysis may be applicable for all cases when determining the importance of the asset. However, the security elements necessary to protect the building can be entirely different, depending on its location. The approach suggests establishing different demarcation points in order to identify sound security strategies. The layers of defense concept proposes that each designer study a particular site and determine critical assets that need to be protected and how protection should take place.

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

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

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

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

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

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

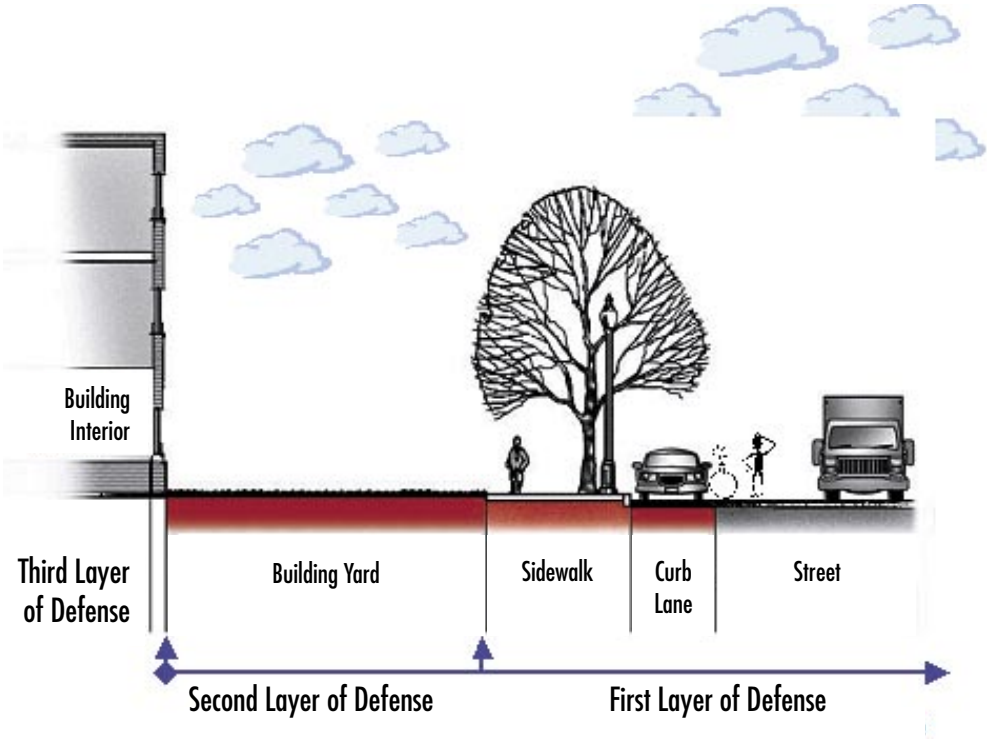


Figure 2-3 Layers of defense in a urban setting

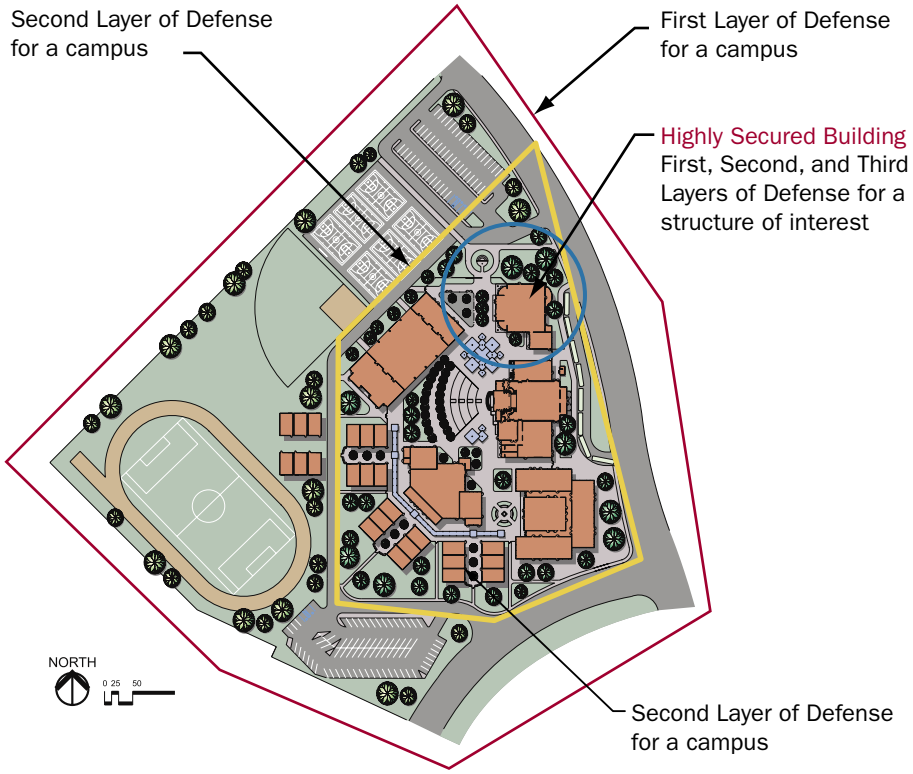


Figure 2-4 Layers of defense when a particular building is considered a critical asset

Identifying the Critical Assets (Task 2.2)

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

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

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

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

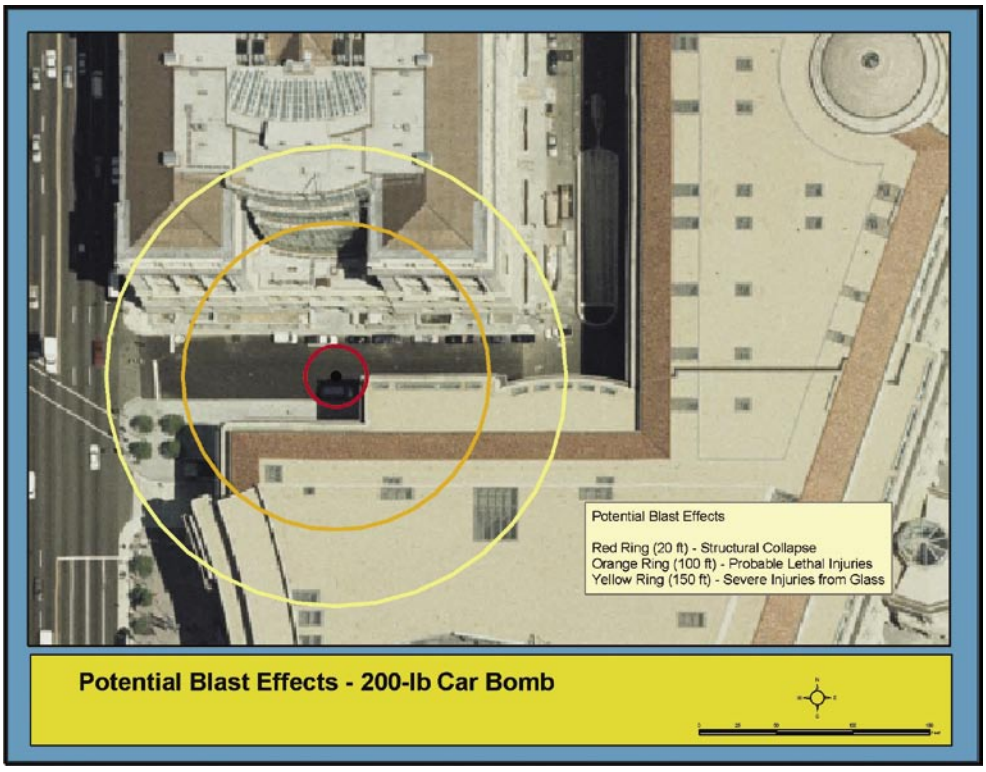


Figure 2-5 Potential blast effects – 200-lb car bomb

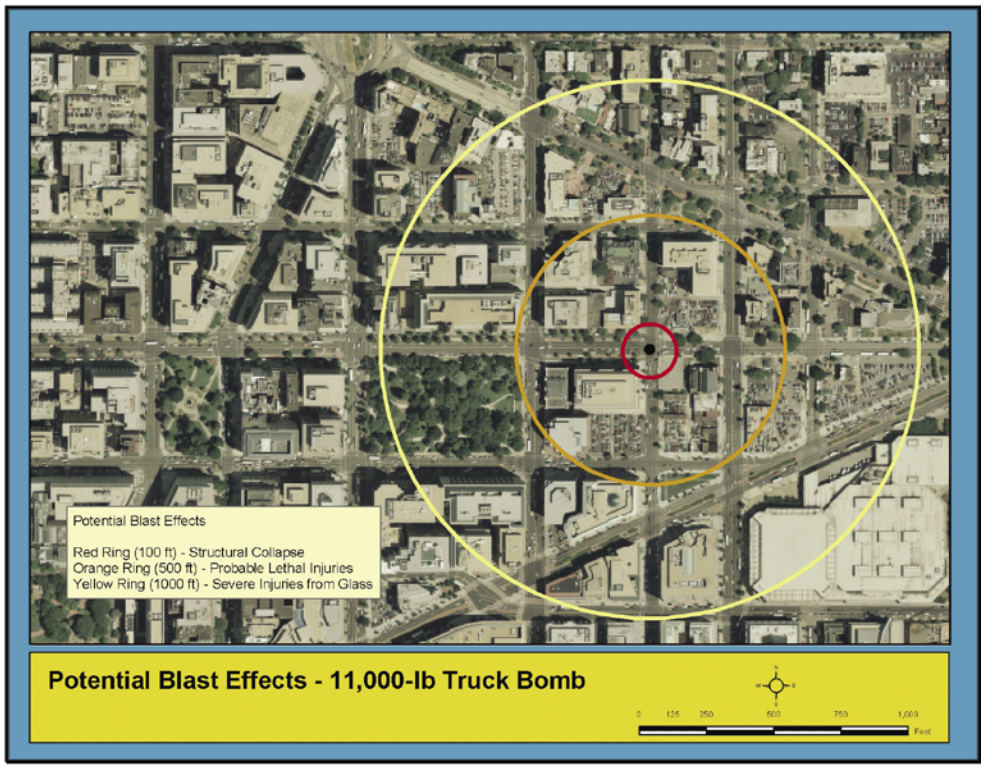
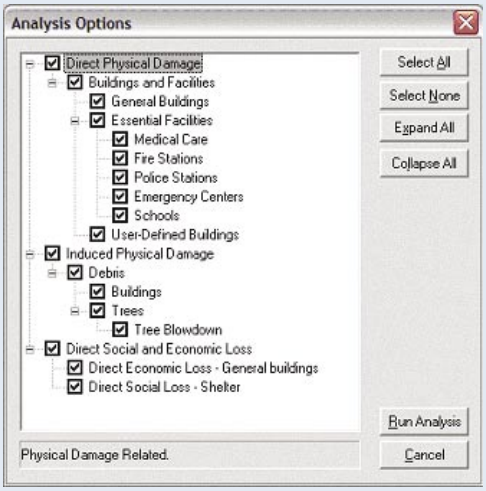


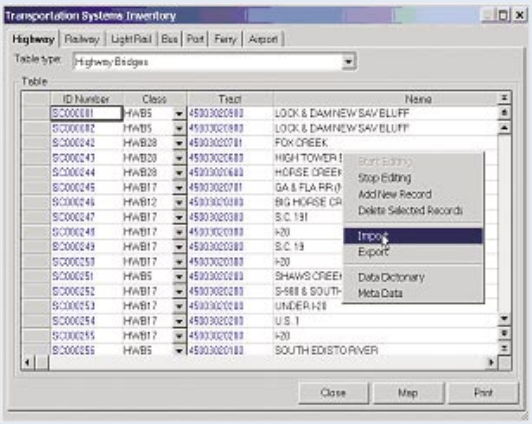
Figure 2-6 Potential blast effects – 11,000-lb truck bomb

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



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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

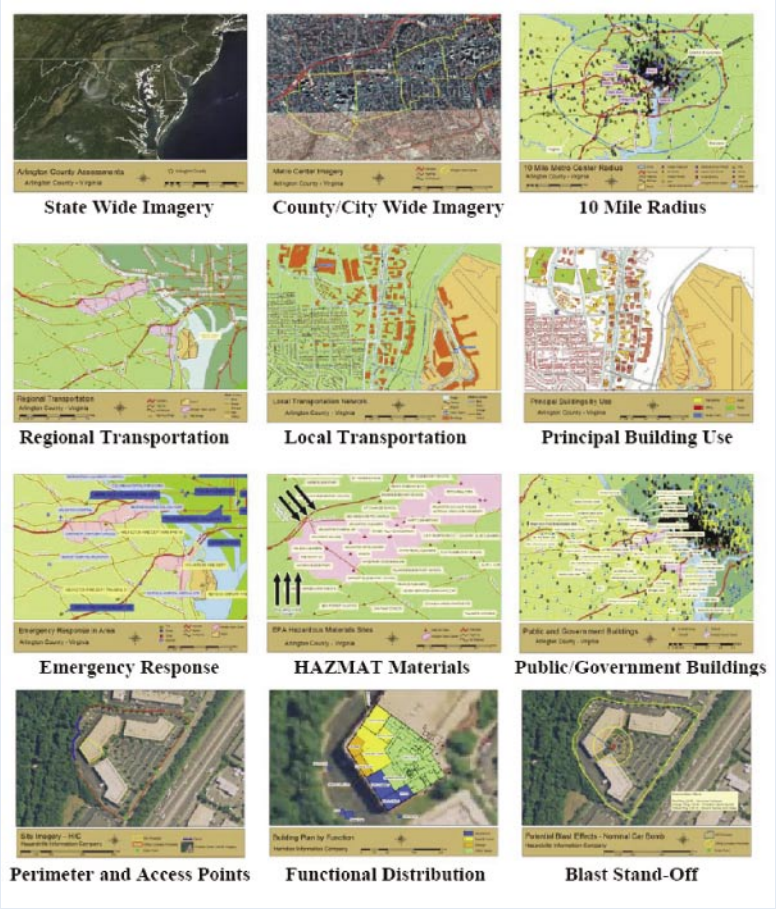


Figure 2-7 Using HAZUS-MH to identify the criticality of assets (continued)

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

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

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

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

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

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

- What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?
- Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)
- Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?
- Is the incoming water supply in a secure location? Is there a secure alternate drinking water supply?
- Are the incoming air intakes in a secure location?
- How much fuel is stored on the site or at the building and how long can this quantity support critical operations? How is it stored? How is it secured?
- Is roof access limited to authorized personnel by means of locking mechanisms?
- What are the types and level of air filtration?
- Are there provisions for air monitors or sensors for CBR agents?

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

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

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

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

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

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

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

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

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

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

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

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

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

Identifying the Building Core Functions and Infrastructure (Task 2.3)

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

Identifying Building Core Functions

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

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

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

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

Table 2-2: Building Core Functions

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

Identifying Building Core Infrastructure

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

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

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

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

Table 2-3: Building Core Infrastructure

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

Levels of Protection

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

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

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

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

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

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

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

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

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

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

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

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

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

Determining the Asset Value Rating (Task 2.4)

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

Table 2-5: Asset Value Scale

Asset Value		
Very High	10	Very High – Loss or damage of the building's assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions.
High	8-9	High – Loss or damage of the building's assets would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time.
Medium High	7	Medium High – Loss or damage of the building's assets would have serious consequences, such as serious injuries or impairment of core processes and functions for an extended period of time.
Medium	5-6	Medium – Loss or damage of the building's assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes.
Medium Low	4	Medium Low – Loss or damage of the building's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes.
Low	2-3	Low – Loss or damage of the building's assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.
Very Low	1	Very Low – Loss or damage of the building's assets would have negligible consequences or impact.

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

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

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

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

The following additional references for blast are recommended:

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

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

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

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

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

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

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

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

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

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

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

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

WORKSHEET 2-1: ASSET VALUE

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

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

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