DUE DILIGENCE: ESTIMATING VULNERABILITY 5

FUNDAMENTAL CHANGES

Vulnerability assessment methodologies developed by DoD and other federal agencies are currently the best available resources for terrorism risk assessment. In order for these resources to be feasible and relevant in commercial buildings, they must be significantly simplified and civilianized.

This chapter provides basic information on the current state of knowledge on the terrorist threat and measures to reduce vulnerability to that threat in commercial buildings. An initial vulnerability estimate process and checklist is proposed. Insurers, lenders, and owners can apply this information to encourage investments in terrorism risk mitigation.

Bringing government experience and expertise regarding terrorism risk and building security to the commercial sector will involve two fundamental changes in the way buildings are designed, managed, and operated, and in the way that due diligence is used to evaluate existing buildings for acquisition or refinancing.

First, businesses will need to carefully evaluate functional aspects of their operations in order to prioritize security requirements. Second, tradeoffs will be required in the level of security provided to ensure continued viability of business operations.

Reducing vulnerability to terrorist threat will involve both physical measures to modify a facility and operational changes. Mitigation will consist mainly of measures to thwart tactics that terrorists might use in attacking organizations and facilities.

DUE DILIGENCE ASSESSMENT OF VULNERABILITY TO TERRORIST ATTACK

Due diligence procedures are employed to assess valuations for property acquisition or financing and to identify risks related to the deal. Such procedures may also be used as part of insurance underwriting. Due diligence often includes both detailed property inspection and rigorous audits of available financial and construction documentation. At the same time, due diligence is a highly specialized field requiring both expertise and extensive prior experience to render sound judgments and recommendations to decision makers.

A Property Condition Assessment (PCA) is used (at levels of detail and rigor appropriate to the investment being considered) as part of due diligence to help make prudent investment decisions. The assessment consists of analysis and assessment of physical conditions of a property by an on-site inspection and review of available construction and operations documentation. Investigators use professional judgment to identify items needing further expert investigation and those that can be readily evaluated by inspection.

Vulnerability to terrorist attack should become a distinct element of due diligence condition assessments in the future. Professionals conducting property condition assessments of vulnerability to terrorist attack must have competency in building systems, operations, and security disciplines.

For terrorism risk and security concerns, a due diligence assessment should also include a property condition assessment investigation of operational procedures and the vulnerability of those procedures to terrorist attack.

MITIGATION OF VULNERABILITY

Strategies for reducing exposure to terrorism risk may be in the form of operational actions or construction projects (either new or existing building renovation). They could include reorganization of land uses, reorientation of roadways, security improvements to site entries, and improvements to the facility, including the existing structure and surrounding site area. For some strategies, the process may include the identification of multiple scenarios, or alternatives, for achieving the desired goal.

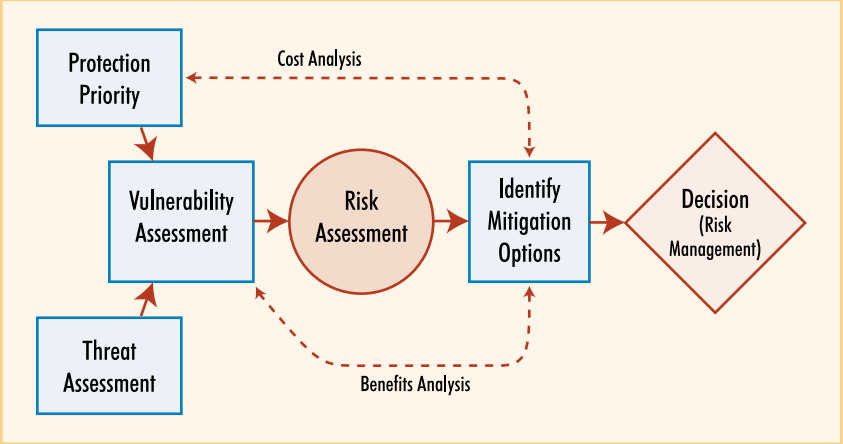
PROCESS MODEL FOR TERRORISM RISK REDUCTION USED IN FEDERAL FACILITIES

United States military services and government agencies have long been involved in assessing vulnerabilities and protecting facilities, especially for off-shore installations. Terrorism and

terrorist attack have been a part of the assessment of threat and vulnerability of government facilities for several decades.

While each government agency has used its own procedures, the general approach has been elaborated and presented in FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*.

Figure 5-1: The Terrorism Risk Reduction Process Model



The terrorism risk reduction process starts with establishment of protection priorities and proceeds to assessment of threats, both providing information to a vulnerability assessment. The vulnerability assessment in turn leads to identification of mitigation options and risk management decisions based on a comparative evaluation of risk, liabilities, and mitigation costs and benefits.

PROTECTION PRIORITY

The first step of the process to assess risk to terrorist attack is to identify the relative importance of the people, business activities, goods, and facilities involved in order to prioritize security actions. This applies to both new and existing facilities. Three actions are recommended in accordance with FEMA 426:

- Define and understand the core functions and processes of the business or institutional entity.

- Identify critical business infrastructure:
  - Critical components (people, functions, and facilities)
  - Critical information systems and data
  - Life safety systems and safe haven areas
  - Security systems
- Assign a relative protection priority, as simple as high, medium, or low, to the occupants, business functions, or physical components of the facility (note that FEMA 426 describes a 9-step scale of values for describing asset values; the 3-step variation presented here is a simplified process):
  - **High Priority.** Loss or damage of the facility 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 Priority.** Loss or damage of the facility would have moderate to serious consequences, such as injuries, or impairment of core functions and processes.
  - **Low Priority.** Loss or damage of the facility would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.

THREAT ASSESSMENT

Military experience indicates that the terrorist threat is from people with the intent to do harm, who are known to exist, have the capability for hostile action, and have expressed the intent to take hostile action.

Threat assessment is a continual process of compiling and examining information concerning potential threats. Information should be gathered from all reliable sources. The assessment process consists of:

- Defining threats

- Identifying likely threat event profiles and tactics

Defining Threats

Defining threats involves analysis of information regarding terrorist existence, capability, history, intention, and targeting:

- **Existence** is the assessment of who is hostile to the organization, or community of concern.
- **Capability** is the assessment of what weapons have been used in carrying out past attacks.
- **History** is the assessment of what the potential terrorist has done in the past and how many times.
- **Intention** is the assessment of what the potential terrorist hopes to achieve.
- **Targeting** is the assessment of the likelihood a terrorist (the specific one may not be known) is performing surveillance on the particular facility, nearby facilities, or facilities that have much in common with the particular organization.

The Homeland Security Advisory System is a color-coded hierarchy of threat conditions. The threat level for a specific business facility could be similarly developed in coordination with local law enforcement, intelligence, and civil authorities.

Table 5-1: Homeland Security Advisory System Related to Threat Analysis Factors

Threat Conditions	Threat Analysis Factors				
	Existence	Capability	History	Intention	Targeting
Severe (Red)	●	●	●	●	●
High (Orange)	●	●	●	●	❍
Elevated (Yellow)	●	●	●	❍	
Guarded (Blue)	●	●	❍		
Low (Green)	●	❍			

LEGEND: ● = Factor must be present. ❍ = Factor may or may not be present.

Adapted from the Commonwealth of Kentucky Office of Homeland Security.

Identifying Likely Threat Event Profiles and Tactics

Identifying the likelihood of specific threats and tactics involves evaluation of attack intentions, hazard event profiles, and the expected effects of an attack on the facility and organization. Table 5-2, based on FEMA 426, presents general event profiles for a range of possible forms of terrorism attack. The profiles describe the mode, duration, and extent of the effects of an attack, as well as mitigating and exacerbating conditions that may exist. These and more specific descriptions can be used to identify threats of concern to individual organizations. (Potential threats are listed in alphabetical order in the table.)

Table 5-2: Event Profiles For Terrorism and Technological Hazards

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
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.
Armed Attack - Ballistics (small arms) - Stand-off weapons (rocket propelled grenades, mortars)	Tactical assault or sniping from remote location.	Generally minutes to days.	Varies, based upon the perpetrators' intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.

Hazard/Threat	Application Mode	Hazard 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.
Biological Agents - 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.	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.

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Chemical Agents - 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.	Chemicals 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 inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target are 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 can protect people and property from harmful effects.
Conventional 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 time duration of the 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.	Energy decreases logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc., can provide shielding by absorbing and/or deflecting energy and debris. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
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.

Hazard/Threat	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Hazardous Material Release (fixed facility 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 can 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.
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 only 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 radiation and radioactive contaminants.
Radiological Agents - 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.

Hazard/Threat	Application Mode	Hazard 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 as it indicates targeting of the facility.	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.
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 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 measures. 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.

Assigning a *Threat Rating*

The ultimate product of a threat assessment is the assignment of a *threat rating* to each hazard of concern to a particular organization. The threat rating, like *protection priority*, is based on expert judgment and may be as simple as high, medium, or low.

- **High Threat.** Known terrorists or hazards, capable of causing loss of or damage to a facility exist. One or more vulnerabilities are present and the terrorists are known or reasonably suspected of having intent to attack the facility.
- **Medium Threat.** Known terrorists or hazards that may be capable of causing loss of or damage to a facility exist. One or

more vulnerabilities may be present. However, the terrorists are not believed to have intent to attack the facility.

- **Low Threat.** Few or no terrorists or hazards exist. Their capability of causing damage to a particular facility is doubtful.

An organization may reasonably be concerned only with high threat ratings in the near term, but may want to consider addressing medium threats over time.

Alternative: Assigning a *Level of Protection Against Threat*

In the absence of experience, assessing terrorist threat is the most difficult aspect of planning to resist terrorist attack. An effective alternative approach may be to select a level of desired protection for a business operation based on management decision-making, and then proceed to a vulnerability assessment. The Department of Defense correlates *levels of protection* with potential damage and expected injuries. The GSA and Interagency Security Committee (ISC) also use the level of protection concept, though the definitions differ slightly. The following levels are based on DoD definitions:

- **High Protection.** Facility superficially damaged; no permanent deformation of primary and secondary structural members or non-structural elements. Only superficial injuries are likely.

- **Medium Protection.** Damaged, but repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Some minor injuries, but fatalities are unlikely.

- **Very Low Protection.** Heavily damaged, onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities.

Note that the 'very low' level is not the same as doing nothing. No action could result in catastrophic building failure and high loss of life.

VULNERABILITY ASSESSMENT

A terrorism vulnerability assessment evaluates any weaknesses that can be exploited by a terrorist. It evaluates the vulnerability of facilities across a broad range of identified threats/hazards and provides a basis for determining physical and operational mitigation measures for their protection. It applies both to new building programming and design and to existing building management and renovation over the service life of a structure.

The useful product of a vulnerability assessment is the assignment of a *vulnerability rating* of all appropriate aspects of building operations and systems to the defined threats for the particular facility. As with protection priority and threat ratings, vulnerability can be cast as high, medium, or low.

- **High Vulnerability.** One or more significant weaknesses have been identified that make the facility highly susceptible to a terrorist or hazard.
- **Medium Vulnerability.** A weakness has been identified that makes the facility somewhat susceptible to a terrorist or hazard.
- **Low Vulnerability.** A minor weakness has been identified that slightly increases the susceptibility of the facility to a terrorist or hazard.

The Building Vulnerability Assessment Checklist, presented in abbreviated form in Appendix B, compiles a comprehensive list of questions to be addressed in assessing the vulnerability of facilities to terrorist attack. A subset of the checklist, discussed in the following section, is particularly useful in the initial screening of existing facilities to identify and prioritize terrorism risk reduction needs. Such an assessment can be integrated into a due

diligence assessment associated with acquisition, refinancing, or insurance underwriting.

INITIAL VULNERABILITY ESTIMATE

Because of the uncertainty of the threat, many insurers, lenders, and owners need a quick, qualitative assessment of the vulnerability of existing buildings to terrorist attack. As experience is gained and more robust vulnerability assessment tools are developed, the rigor of data collection and analysis will increase. For now, the estimate of vulnerability to a simple qualitative scale (high, medium, or low as defined by the vulnerability ratings described above) may provide useful information.

> *"There are no universal solutions to preclude terrorist attacks, since the threat is largely unpredictable and certainly will change over time."*
>
> (Installation Force Protection Guidelines, USAF)
>
> *"No matter how many measures are implemented risk is always present."*
>
> (Structural Engineering Guidelines for New Embassy Office Buildings, U.S. Department of State, Bureau of Diplomatic Security)

Answering even basic questions concerning vulnerability to terrorist attack may involve three means of data collection:

- Visual inspection
- Document review
- Organization and management procedures review

Visual Inspection

A property condition assessment of vulnerability to terrorist attack includes an onsite visual inspection encompassing evaluation of the site and all facility systems including architectural, structural, building envelope, utility, mechanical, plumbing and gas, electrical, fire alarm, communications and information technology systems. Equipment operations and maintenance procedures and records and security systems, planning, and procedures should also be scrutinized. The investigation may need to go beyond the site to vulnerability of utility and other infrastructure systems.

Design Documents Review

The on-site inspection team should work with the property owner to obtain plans, specifications and related construction documents as necessary. Equipment operation and maintenance procedures and records as well as security procedures should also be scrutinized. All documents should be reviewed assessing concerns related to terrorism vulnerability.

Organization and Management Procedures Review

Because of the transitory nature of the terrorist threat and its uncertain duration, the most effective approaches to terrorism risk reduction in facilities may emphasize reorganization of operational functions and procedures rather than modification of physical systems. The vulnerability assessment team must scrutinize business and operational practices to identify opportunities to reduce exposure to attack. This will involve scrutinizing both owner and tenant operations at the building site.

Assessment of Vulnerability to Expected Methods and Means of Attack

Each building system and business procedure should be assessed on its vulnerability to a range of terrorist attack methods and means.

Based on military experience, common terrorist tactics include the use of moving or stationary vehicles, covert entry, and/or disguise in mail or shipping materials to deliver destructive weapons.

At present, terrorist attacks might include blast effects, airborne contamination, waterborne contamination, or some combination of attack mechanisms. For additional information, see FEMA 426 and FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks.*

VULNERABILITY ESTIMATE SCREENING

The following screening tool tables provide guidance for initial vulnerability assessment. The intention of this assessment is to distinguish facilities of high, medium, or low vulnerability to terrorist attack. The implication is that high vulnerability facilities should receive more detailed analysis. Specific strategies for risk reduction should be developed.

These quick, qualitative 'vulnerability estimate' questions were selected from the Building Vulnerability Assessment Checklist in FEMA 426. Each question is characterized by how information concerning the question will likely be collected (visual inspection, design documentation, and/or review of organizational/management procedures), and common terrorist attack tactics (delivery by moving, stationary vehicles, or covert entry, disguised in the mail or in supply materials; and blast pressure, airborne, or waterborne attack mechanisms).

For this initial assessment, subjective ratings by qualified professionals familiar with the facility are appropriate. Assigning a "high, medium, or low" vulnerability rating to the responses to vulnerability questions for each building system will provide a solid preliminary basis for estimating the overall vulnerability of a particular facility to terrorist attack. The answers to the questions will also indicate areas of opportunity for mitigation actions to reduce terrorism risk.

'Site' Questions

A vulnerability assessment of the 'Site' will look at surrounding structures, terrain, perimeter controls, traffic patterns and separations, landscaping elements and features, lines of site, etc.

'Site' questions focus primarily on visual inspection to develop ratings. The questions emphasize vulnerability to moving vehicle, stationary vehicle, and covert entry tactics. Vulnerability to blast is the primary concern addressed.

Table 5-3a: FEMA 'Site Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What major structures surround the facility?	❑	●	●									
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?	❑	●	●									
What are the site access points to the facility?	❑	●			●		●					
What is the minimum distance from the inspection location to the building?	❑	●			●		●			●		
Is there any potential access to the site or facility through utility paths or water runoff?	❑	●	●				●					
What are the existing types of vehicle anti-ram devices for the facility?	❑	●			●					●		
What is the anti-ram buffer zone standoff distance from the building to unscreened vehicles or parking?	❑	●			●							
Are perimeter barriers capable of stopping vehicles?	❑	●	●		●							
Does site circulation prevent high-speed approaches by vehicles?	❑	●			●							
Is there a minimum setback distance between the building and parked vehicles?	❑	●				●				●		
Does adjacent surface parking maintain a minimum standoff distance?	❑	●				●				●		
Do site landscaping and street furniture provide hiding places?	❑	●					●					

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Architectural' Questions

Assessing 'Architectural' vulnerability will investigate tenancy, services, public and private access, access controls, activity patterns, exposures, etc.

'Architectural' questions focus equally on visual inspection and evaluation of organizational and management procedures to develop ratings. The questions emphasize vulnerability to moving vehicle, stationary vehicle, and covert entry tactics. Vulnerability to blast is the primary expressed concern.

Table 5-3b: FEMA 'Architectural Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What major structures surround the facility?	❑	●	●	●								
Do entrances avoid significant queuing?	❑	●		●								
What are the adjacent land uses immediately outside the perimeter of this facility?	❑	●		●								
Are public and private activities separated?	❑	●					●					
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 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?	❑	●	●	●						●		
Is high visitor activity away from critical assets?	❑			●			●					
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?	❑			●								
Do interior barriers differentiate level of security within a facility?	❑	●	●	●								
Are emergency systems located away from high-risk areas?	❑	●	●	●								

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Structural and Building Envelope Systems' Questions

A vulnerability assessment of 'Structural Systems' will look at construction type, materials, detailing, collapse characteristics, critical elements, etc. An assessment of 'Building Envelope' will involve investigating strength, fenestration, glazing characteristics and detailing, anchorage, etc.

'Structural and Building Envelop Systems' questions rely on review of construction documents and visual inspection to develop ratings. Vulnerability to blast is the primary concern.

Table 5-3c:
FEMA 'Structural & Building Envelope Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What type of construction?	❑	●	●							●		
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?	❑	●	●							●		
Is the structure vulnerable to progressive collapse?	❑	●	●									
Are there adequate redundant load paths in the structure?	❑	●	●							●		
What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	❑		●							●		

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Utility Systems' Questions

A vulnerability assessment of 'Utility Systems' will look at the full range of source and supply systems serving the facility including water, fuel, and electricity supply; fire alarm and suppression, communications, etc.

'Utility Systems' questions rely equally on information obtained from visual inspection, review of construction documents, and organizational and management procedures to develop ratings. Vulnerability to waterborne contaminants is expressly considered.

Table 5-3d: FEMA 'Utility Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)	❑	●	●									●
How many gallons and how long will it allow operations to continue?	❑	●	●	●								●
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?	❑	●	●	●								
Are the sprinkler and standpipe connections adequate and redundant?	❑	●	●									
What fuel supplies do the facility rely upon for critical operation?	❑	●	●	●								
Where is the fuel supply obtained?	❑			●								
Are there alternate sources of fuel?	❑			●								
Can alternate fuels be used?	❑		●	●								
What is the normal source of electrical service for the facility?	❑	●	●									
What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested?	❑	●	●	●								
By what means does the main telephone and data communications interface the facility?	❑	●	●	●								

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Mechanical Systems' Questions

A vulnerability assessment of 'Mechanical Systems' will investigate air supply and exhaust configurations, filtration, sensing and monitoring, system zoning and control, elevator management, etc.

'Mechanical Systems' vulnerability questions and ratings rely primarily on information obtained from review of construction documents and visual inspection. Vulnerability to airborne contaminants is the primary consideration, including contamination from Chemical, Biological, and Radiological attack.

Table 5-3e: FEMA 'Mechanical Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure)	❑	●	●									●
Are there multiple air intake locations?	❑	●	●									●
How are air handling systems zoned?	❑	●	●									●
Are there large central air handling units or are there multiple units serving separate zones?	❑		●									●
Are there any redundancies in the air handling system?	❑		●	●								●
Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)	❑	●										

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Plumbing and Gas Systems' Questions

A vulnerability assessment of 'Plumbing and Gas Systems' will look at the liquid distribution systems serving the facility including water and fuel distribution, water heating, fuel storage, etc.

'Plumbing and Gas Systems' questions rely primarily on information from review of construction documents to develop ratings. Vulnerability to waterborne contaminants is expressly considered.

Table 5-3f: FEMA 'Plumbing & Gas Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
What is the method of water distribution?	❑		●									●
What is the method of gas distribution? (heating, cooking, medical, process)	❑		●									
What is the method of heating domestic water?	❑	●	●	●								
Are there reserve supplies of critical gases?	❑		●	●								

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Electrical Systems' Questions

A vulnerability assessment of 'Electrical Systems' will evaluate transformer and switchgear security, electricity distribution and accessibility, emergency systems, etc.

'Electrical Systems' questions primarily on information from visual inspection and review of construction documents to develop ratings. No particular attack mechanism is emphasized.

Table 5-3g: FEMA 'Electrical Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Are there any transformers or switchgears located outside the building or accessible from the building exterior?	❑	●										
Are they (transformers or switchgears) vulnerable to public access?	❑	●										
Are critical electrical systems located in areas outside of secured electrical areas?	❑	●	●	●								
Does emergency backup power exist for all areas within the facility or for critical areas only?	❑	●	●									

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Fire Alarm Systems' Questions

A vulnerability assessment of 'Fire Alarm Systems' will look at detection sensing and signaling, system configurations, accessibility of controls, redundancies, etc.

'Fire Alarm Systems' questions rely both on information from review of construction documents and review of organizational and management procedures to develop ratings. No particular attack mechanism is emphasized.

Table 5-3h: FEMA 'Fire Alarm Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Is the fire alarm system stand-alone or integrated with other functions such as security and environmental or building management systems?	❑		●	●								
Is there redundant off-premises fire alarm reporting?	❑		●	●								

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

'Communications and Information Technology Systems' Questions

A vulnerability assessment of 'Communications and Information Technology Systems' will evaluate distribution, power supplies, accessibility, control, notification, backups, etc.

'Communications and Information Technology Systems' questions rely on information from visual inspection, review of construction documents, and review of organizational and management procedures to develop ratings. No particular attack mechanism is emphasized.

Table 5-3i: FEMA 'Communication and IT Systems' Vulnerability Estimate

	Vulnerability Rating (H, M, L)	Visual inspection	Document review	Org/Mgmt procedure	Moving vehicle	Stationary vehicle	Covert entry	Mail	Supplies	Blast effects	Airborne (contamination)	Waterborne (contamination)
Where is the main telephone distribution room and where is it in relation to higher risk areas?	❑	●	●	●								
Where are communication systems wiring closets located? (voice, data, signal, alarm)	❑	●	●									

LEGEND: ❑ = Determine high, medium, or low vulnerability rating. ● = Applicability of factor to question.

ADDITIONAL SOURCES OF DETAILED FACILITY INFORMATION

The foregoing questions provide a framework for a qualitative estimate of facility vulnerability to terrorist attack. A more detailed and quantitative evaluation will involve significantly more review of information in all areas, including additional information concerning 'Equipment Operations and Maintenance' (up to date drawings, manuals, and procedures, training, monitoring, etc.); 'Security Systems' (perimeter and interior sensing, monitoring, and control, security system documentation and training, etc.); and the 'Security Master Plan' (currency, responsibilities, etc.).

Appendix B presents the complete list of detailed questions from FEMA 426 that should be considered in fully evaluating vulnerability to terrorist threats. The means of data collection that should be employed and the particular terrorist tactics and attack mechanisms addressed by each question are identified in the appendix so that specialized checklists can be created to assess vulnerability to terrorist tactics of particular concern to an individual organization.

VULNERABILITY REDUCTION COST INFORMATION AND ESTIMATES

Typically, a property condition assessment for due diligence would be followed by consideration of the anticipated costs and timing of needed upgrades of facility systems. Certainly, estimates of expected costs of mitigation of system vulnerability to terrorist attack will become important at some point in the decision-making process.

However, an assessment using the questions described above does not include the level of information needed to project costs. The qualitative analysis described simply determines broad preliminary options for reducing terrorism risk in a particular existing facility and does not give insight to expected costs of risk reduction. At some point in the future, fully capable due dili-

gence tools for assessing vulnerability to terrorist attack will very likely include such information and detail. For further discussion of costs related to blast mitigation, see FEMA 427, Chapter 8.