

APPENDIX A: BUILDING VULNERABILITY ASSESSMENT CHECKLIST

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

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

Section	Vulnerability Question	Guidance	Observations
1	Site		
1.1	<p>What major structures surround the facility (site or building(s))?</p> <p>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)?</p> <p>What are the adjacent land uses immediately outside the perimeter of this facility (site or building(s))?</p>	<p>Critical infrastructure to consider includes:</p> <p>Telecommunications infrastructure</p> <p>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</p> <p>Electric power systems</p> <p>Power plants, especially nuclear facilities; transmission and distribution system components; fuel distribution, delivery, and storage</p> <p>Gas and oil facilities</p> <p>Hazardous material facilities, oil/gas pipelines, and storage facilities</p>	

Section	Vulnerability Question	Guidance	Observations
1	Site		
	<p>Do future development plans change these land uses outside the facility (site or building (s)) perimeter?</p> <p>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.</p>	<p>Banking and finance institutions</p> <p>Financial institutions (banks, credit unions) and the business district; note schedule business/financial district may follow; armored car services</p> <p>Transportation networks</p> <p>Airports: carriers, flight paths, and airport layout; location of air traffic control towers, runways, passenger terminals, and parking areas</p> <p>Bus Stations</p> <p>Pipelines: oil; gas</p> <p>Trains/Subways: rails and lines, railheads/rail yards, interchanges, tunnels, and cargo/passenger terminals; note hazardous material transported</p> <p>Traffic: interstate highways/roads/tunnels/bridges carrying large volumes; points of congestion; note time of day and day of week</p> <p>Trucking: hazardous materials cargo loading/unloading facilities; truck terminals, weigh stations, and rest areas</p> <p>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)</p> <p>Water supply systems</p> <p>Pipelines and process/treatment facilities, dams for water collection; wastewater treatment</p> <p>Government services</p> <p>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)</p> <p>Emergency services</p> <p>Backup facilities, communications centers, Emergency Operations Centers (EOCs), fire/Emergency Medical Service (EMS) facilities, Emergency Medical Center (EMCs), law enforcement facilities</p>	

Section	Vulnerability Question	Guidance	Observations
1	Site	<p>The following are not critical infrastructure, but have potential collateral damage to consider:</p> <p>Agricultural facilities: chemical distribution, storage, and application sites; crop spraying services; farms and ranches; food processing, storage, and distribution facilities</p> <p>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</p> <p>Events and attractions: festivals and celebrations; open-air markets; parades; rallies, demonstrations, and marches; religious services; scenic tours; theme parks</p> <p>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</p> <p>Political or symbolically significant sites: embassies, consulates, landmarks, monuments, political party and special interest groups offices, religious sites</p> <p>Public/private institutions: academic institutions, cultural centers, libraries, museums, research facilities and laboratories, schools</p> <p>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</p> <p>References: <i>FEMA 386-7, FEMA SLG 101, DOJ NCJ181200</i></p>	
1.2	Does the terrain place the building in a depression or low area?	<p>Depressions or low areas can trap heavy vapors, inhibit natural decontamination by prevailing winds, and reduce the effectiveness of in-place sheltering.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	

Section	Vulnerability Question	Guidance	Observations
1	Site		
1.3	In dense, urban areas, does curb lane parking allow uncontrolled vehicles to park unacceptably close to a building in public rights-of-way?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.4	Is a perimeter fence or other types of barrier controls in place?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.5	What are the site access points to the site or building?	<p>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.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.6	Is vehicle traffic separated from pedestrian traffic on the site?	<p>Pedestrian access should not be endangered by car traffic. Pedestrian access, especially from public transportation, should not cross vehicle traffic if possible.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
1.7	Is there vehicle and pedestrian access control at the perimeter of the site?	<p>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.</p> <p>Control on-site parking with identification checks, security personnel, and access control systems.</p> <p>Reference: <i>FEMA 386-7</i></p>	

Section	Vulnerability Question	Guidance	Observations
1	Site		
1.8	<p>Is there space for inspection at the curb line or outside the protected perimeter?</p> <p>What is the minimum distance from the inspection location to the building?</p>	<p>Design features for the vehicular inspection point include: vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and prevent tailgating.</p> <p>If screening space cannot be provided, consider other design features such as: hardening and alternative location for vehicle search/inspection.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.9	<p>Is there any potential access to the site or building through utility paths or water runoff?</p>	<p>Eliminate potential site access through utility tunnels, corridors, manholes, stormwater runoff culverts, etc. Ensure covers to these access points are secured.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.10	<p>What are the existing types of vehicle anti-ram devices for the site or building?</p> <p>Are these devices at the property boundary or at the building?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.11	<p>What is the anti-ram buffer zone stand-off distance from the building to unscreened vehicles or parking?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.12	<p>Are perimeter barriers capable of stopping vehicles?</p> <p>Will the vehicle barriers at the perimeter and building maintain access for emergency responders, including large fire apparatus?</p>	<p>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.</p> <p>References: <i>Military Handbook 1013/14 and GSA PBS P-100</i></p>	

Section	Vulnerability Question	Guidance	Observations
1	Site		
1.13	Does site circulation prevent high-speed approaches by vehicles?	The intent is to use site circulation to minimize vehicle speeds and eliminate direct approaches to structures. Reference: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	
1.18	Are garage or service area entrances for employee-permitted vehicles protected by suitable anti-ram devices? Coordinate this protection with other anti-ram devices, such as on the perimeter or property boundary to avoid duplication of arresting capability.	Control internal building parking, underground parking garages, and access to service areas and loading docks in this manner with proper access control, or eliminate the parking altogether. The anti-ram device must be capable of arresting a vehicle of the designated threat size at the speed attainable at the location.	

Section	Vulnerability Question	Guidance	Observations
1	Site		
1.19	Do site landscaping and street furniture provide hiding places?	<p>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.</p> <p>If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.20	Is the site lighting adequate from a security perspective in roadway access and parking areas?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
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?	<p>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.</p> <p>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.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.22	Do signs provide control of vehicles and people?	<p>The signage should be simple and have the necessary level of clarity. However, signs that identify sensitive areas should generally not be provided.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.23	Are all existing fire hydrants on the site accessible?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	

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?	<p>The focus of CPTED is on creating defensible space by employing:</p> <ol style="list-style-type: none"> 1. Natural access controls: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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. <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	

Section	Vulnerability Question	Guidance	Observations
2	Architectural		
2.2	Is it a mixed-tenant building?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.3	Are pedestrian paths planned to concentrate activity to aid in detection?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.4	Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	<p>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.</p> <p>References: <i>USAF Installation Force Protection Guide and DoD UCF 4-010-01</i></p>	
2.5	Do entrances avoid significant queuing?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.6	<p>Does security screening cover all public and private areas?</p> <p>Are public and private activities separated?</p> <p>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?</p>	<p>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.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	

Section	Vulnerability Question	Guidance	Observations
2	Architectural		
2.7	<p>Is access control provided through main entrance points for employees and visitors?</p> <p>(lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)</p>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
2.8	<p>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.?</p>	<p>Finishes and signage should be designed for visual simplicity.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.9	<p>Is access to elevators distinguished as to those that are designated only for employees and visitors?</p>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
2.10	<p>Do public and employee entrances include space for possible future installation of access control and screening equipment?</p>	<p>These include walk-through metal detectors and x-ray devices, identification check, electronic access card, search stations, and turnstiles.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.11	<p>Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?</p>	<p>Consider for exterior entrances to the building or to access critical areas within the building if explosive blast hazard must be mitigated.</p> <p>Reference: <i>U.S. Army TM 5-853</i></p>	
2.12	<p>Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.13	<p>Do circulation routes have unobstructed views of people approaching controlled access points?</p>	<p>This applies to building entrances and to critical areas within the building.</p> <p>References: <i>USAF Installation Force Protection Guide and DoD UFC 4-010-01</i></p>	

Section	Vulnerability Question	Guidance	Observations
2	Architectural		
2.14	Is roof access limited to authorized personnel by means of locking mechanisms?	References: <i>GSA PBS-P100 and CDC/NIOSH, Pub 2002-139</i>	
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?	<p>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.</p> <p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
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?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.17	Is high visitor activity away from critical assets?	<p>High-risk activities should also be separated from low-risk activities. Also, visitor activities should be separated from daily activities.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
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: <i>USAF Installation Force Protection Guide</i>	

Section	Vulnerability Question	Guidance	Observations
2 Architectural			
2.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/ alarm systems, fire suppression water mains, cooling and heating mains, etc.?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.20	<p>Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets?</p> <p>Is the mailroom located near the loading dock?</p>	<p>The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief.</p> <p>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.</p> <p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.21	Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?	<p>Screening of all deliveries to the building, including U.S. mail, commercial package delivery services, delivery of office supplies, etc.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.22	Are areas of refuge identified, with special consideration given to egress?	<p>Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards.</p> <p>Reference: <i>FEMA 386-7</i></p>	
2.23	<p>Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur?</p> <p>Are stairways maintained with positive pressure or are there other smoke control systems?</p>	<p>Consider designing stairs so that they discharge into areas other than lobbies, parking, or loading docks.</p> <p>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.</p> <p>References: <i>GSA PBS-P100 and CDC/NIOSH, Pub 2002-139</i></p>	

Section	Vulnerability Question	Guidance	Observations
2	Architectural		
2.24	Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?	Egress pathways should be hardened and discharge into safe areas. Reference: <i>FEMA 386-7</i>	
2.25	Do interior barriers differentiate level of security within a building?	Reference: <i>USAF Installation Force Protection Guide</i>	
2.26	Are emergency systems located away from high-risk areas?	The intent is to keep the emergency systems out of harm's way, such that one incident does not take out all capability – both the regular systems and their backups. Reference: <i>FEMA 386-7</i>	
2.27	Is interior glazing near high-risk areas minimized? Is interior glazing in other areas shatter-resistant?	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. Reference: <i>GSA PBS-P100</i>	
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: <i>DoD UCF 4-101-01</i>	

Section	Vulnerability Question	Guidance	Observations
3	Structural Systems		
3.1	<p>What type of construction?</p> <p>What type of concrete and reinforcing steel?</p> <p>What type of steel?</p> <p>What type of foundation?</p>	<p>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.</p> <ul style="list-style-type: none"> 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 <p>References: <i>FEMA 154 and Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
3.2	<p>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?</p>	<p>Reference: <i>GSA PBS-P100</i></p>	

Section	Vulnerability Question	Guidance	Observations
3	Structural Systems		
	<p>Do the lap splices fully develop the capacity of the reinforcement?</p> <p>Are lap splices and other discontinuities staggered?</p> <p>Do the connections possess ductile details?</p> <p>Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?</p>		
3.3	<p>Are the steel frame connections moment connections?</p> <p>Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system?</p> <p>What are the floor-to-floor heights?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.4	<p>Are critical elements vulnerable to failure?</p>	<p>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.</p> <p>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.</p> <p>Secondary Structural Elements consist of all other load-bearing members, such as floor beams, slabs, etc.</p> <p>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.</p> <p>Secondary Non-Structural Elements consist of all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures.</p> <p>Reference: <i>GSA PBS-P100</i></p>	

Section	Vulnerability Question	Guidance	Observations
3	Structural Systems		
3.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?	<p>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:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Reference: <i>DoD UFC 4-010-01</i></p>	
3.6	<p>Is the structure vulnerable to progressive collapse?</p> <p>Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?</p> <p>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?</p>	<p>Design to mitigate progressive collapse is an independent analysis to determine a system’s ability to resist structural collapse upon the loss of a major structural element or the system’s ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted.</p> <p>Reference: <i>GSA PBS-P100</i></p>	

Section	Vulnerability Question	Guidance	Observations
3	Structural Systems		
	<p>Do architectural or structural features provide a minimum 6-inch stand-off to the internal columns (primary vertical load carrying members)?</p> <p>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?</p>		
3.7	Are there adequate redundant load paths in the structure?	<p>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.</p> <p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.8	Are there transfer girders supported by columns within unscreened public spaces or at the exterior of the building?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.9	What is the grouting and reinforcement of masonry (brick and/or concrete masonry unit (CMU)) exterior walls?	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i> recommends fully grouted and reinforced CMU construction where CMU is selected.</p>	

Section	Vulnerability Question	Guidance	Observations
3	Structural Systems		
		Reference: <i>DoD Minimum Antiterrorism Standards for Buildings</i> 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: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	

Section	Vulnerability Question	Guidance	Observations
4	Building Envelope		
4.2	<p>Is there less than a 40 percent fenestration opening per structural bay?</p> <p>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.)</p> <p>Do the glazing systems with a ½-inch (¾-inch is better) bite contain an application of structural silicone?</p> <p>Is the glazing laminated or is it protected with an anti-shatter (fragment retention) film?</p> <p>If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?</p>	<p>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.</p> <p>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.</p> <p>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).</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.3	<p>Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected?</p> <p>Are the walls capable of withstanding the dynamic reactions from the windows?</p> <p>Will the anchorage remain attached to the walls of the building during an explosive event without failure?</p> <p>Is the façade connected to backup block or to the structural frame?</p> <p>Are non-bearing masonry walls reinforced?</p>	<p>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.</p> <p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.4	<p>Does the building contain ballistic glazing?</p>	<p>Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material.</p>	

Section	Vulnerability Question	Guidance	Observations
4	Building Envelope		
	<p>Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing?</p> <p>Does the building contain security-glazing?</p> <p>Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material?</p> <p>Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.5	<p>Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?</p>	<p>n-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures.</p> <p>These non-window openings should also be as secure as the rest of the building envelope against forced entry.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
5	Utility Systems		
5.1	<p>What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)</p> <p>Is there a secure alternate drinking water supply?</p>	<p>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.</p> <p>Reference: <i>FEMA 386-7</i></p>	
5.2	<p>Are there multiple entry points for the water supply?</p>	<p>If the building or site has only one source of water entering at one location, the entry point should be secure.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
5.3	<p>Is the incoming water supply in a secure location?</p>	<p>Ensure that only authorized personnel have access to the water supply and its components.</p> <p>Reference: <i>FEMA 386-7</i></p>	
5.4	<p>Does the building or site have storage capacity for domestic water?</p> <p>How many gallons of storage capacity are available and how long will it allow operations to continue?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities.</i></p>	

Section	Vulnerability Question	Guidance	Observations
5	Utility Systems		
5.5	<p>What is the source of water for the fire suppression system? (local utility company lines, storage tanks with utility company backup, lake, or river)</p> <p>Are there alternate water supplies for fire suppression?</p>	<p>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.</p> <p>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.</p> <p>Reference: <i>FEMA 386-7</i></p>	
5.6	<p>Is the fire suppression system adequate, code-compliant, and protected (secure location)?</p>	<p>Standpipes, water supply control valves, and other system components should be secure or supervised.</p> <p>Reference: <i>FEMA 386-7</i></p>	
5.7	<p>Do the sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation?</p> <p>Are the sprinkler and standpipe connections adequate and redundant?</p> <p>Are there fire hydrant and water supply connections near the sprinkler/standpipe connections?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
5.8	<p>Are there redundant fire water pumps (e.g., one electric, one diesel)?</p> <p>Are the pumps located apart from each other?</p>	<p>Collocating fire water pumps puts them at risk for a single incident to disable the fire suppression system.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
5.9	<p>Are sewer systems accessible?</p> <p>Are they protected or secured?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.10	<p>What fuel supplies do the building rely upon for critical operation?</p>	<p>Typically, natural gas, propane, or fuel oil are required for continued operation.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
5	Utility Systems		
5.11	How much fuel is stored on the site or at the building and how long can this quantity support critical operations? How is it stored? How is it secured?	Fuel storage protection is essential for continued operation. Main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals). References: <i>GSA PBS-P100 and Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.17	Is the incoming electric service to the building secure?	Typically, the service entrance is a locked room, inaccessible to the public. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Section	Vulnerability Question	Guidance	Observations
5	Utility Systems		
5.18	<p>What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested?</p> <p>Is the emergency power collocated with the commercial electric service?</p> <p>Is there an exterior connection for emergency power?</p>	<p>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.</p> <p>Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
5.19	By what means do the main telephone and data communications interface the site or building?	<p>Typically, communication ducts or other conduits are available. Overhead service is more identifiable and vulnerable.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.20	Are there multiple or redundant locations for the telephone and communications service?	<p>Secure locations of communications wiring entry to the site or building are required.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.21	<p>Does the fire alarm system require communication with external sources?</p> <p>By what method is the alarm signal sent to the responding agency: telephone, radio, etc.?</p> <p>Is there an intermediary alarm monitoring center?</p>	<p>Typically, the local fire department responds to an alarm that sounds at the station or is transmitted over phone lines by an auto dialer.</p> <p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.22	Are utility lifelines aboveground, underground, or direct buried?	<p>Utility lifelines (water, power, communications, etc.) can be protected by concealing, burying, or encasing.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	

Section	Vulnerability Question	Guidance	Observations
6	Mechanical Systems (HVAC and CBR)		
6.1	<p>Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure)</p> <p>Are the intakes and exhausts accessible to the public?</p>	<p>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.</p> <p>Reference: <i>GSA PBS-P100</i> 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.</p> <p>Reference: <i>DoD UFC 4-010-01</i> 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.</p> <p>Reference: <i>CDC/NIOSH, Pub 2002-139</i> 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".</p> <p>Reference: <i>LBNL PUB-51959</i>: Exhausts are also a concern 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).</p>	
6.2	<p>Is roof access limited to authorized personnel by means of locking mechanisms?</p> <p>Is access to mechanical areas similarly controlled?</p>	<p>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.</p> <p>References: <i>GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959</i></p>	
6.3	Are there multiple air intake locations?	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
6.4	What are the types of air filtration? Include the efficiency and number of filter modules for	<p>MERV – Minimum Efficiency Reporting Value</p> <p>HEPA – High Efficiency Particulate Air</p>	

Section	Vulnerability Question	Guidance	Observations
6 Mechanical Systems (HVAC and CBR)			
	<p>each of the main air handling systems?</p> <p>Is there any collective protection for chemical, biological, and radiological contamination designed into the building?</p>	<p>Activated charcoal for gases</p> <p>Ultraviolet C for biologicals</p> <p>Consider mix of approaches for optimum protection and cost-effectiveness.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.5	Is there space for larger filter assemblies on critical air handling systems?	<p>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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.6	Are there provisions for air monitors or sensors for chemical or biological agents?	<p>Duct mounted sensors are usually 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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.7	By what method are air intakes and exhausts closed when not operational?	<p>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.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.8	<p>How are air handling systems zoned?</p> <p>What areas and functions do each of the primary air handling systems serve?</p>	<p>Understanding the critical areas of the building that must continue functioning focuses security and hazard mitigation measures.</p> <p>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.</p> <p>Conversely, emergency egress routes should receive positive pressurization to ensure contamination does not hinder egress. Consider filtering of the pressurization air.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.9	Are there large central air handling units or are there multiple units serving separate zones?	<p>Independent units can continue to operate if damage occurs to limited areas of the building.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
6 Mechanical Systems (HVAC and CBR)			
6.10	<p>Are there any redundancies in the air handling system?</p> <p>Can critical areas be served from other units if a major system is disabled?</p>	<p>Redundancy reduces the security measures required compared to a non-redundant situation.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
6.11	<p>Is the air supply to critical areas compartmentalized?</p> <p>Similarly, are the critical areas or the building as a whole, considered tight with little or no leakage?</p>	<p>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.</p> <p>Smoke testing of the air supply to critical areas may be necessary.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.12	<p>Are supply, return, and exhaust air systems for critical areas secure?</p> <p>Are all supply and return ducts completely connected to their grilles and registers and secure?</p> <p>Is the return air not ducted?</p>	<p>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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.13	<p>What is the method of temperature and humidity control?</p> <p>Is it localized or centralized?</p>	<p>Central systems can range from monitoring only to full control. Local control may be available to override central operation.</p> <p>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).</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
6.14	<p>Where are the building automation control centers and cabinets located?</p>	<p>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.</p>	

Section	Vulnerability Question	Guidance	Observations
6	Mechanical Systems (HVAC and CBR)		
	<p>Are they in secure areas?</p> <p>How is the control wiring routed?</p>	<p>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.</p> <p>References: <i>FEMA 386-7, DOC CIAO Vulnerability Assessment Framework 1.1 and LBNL Pub 51959</i></p>	
6.15	<p>Does the control of air handling systems support plans for sheltering in place or other protective approach?</p>	<p>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.</p> <p>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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.16	<p>Are there any smoke evacuation systems installed?</p> <p>Does it have purge capability?</p>	<p>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.</p> <p>References: <i>GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959</i></p>	
6.17	<p>Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)</p>	<p>Roof-mounted equipment should be kept away from the building perimeter.</p> <p>Reference: <i>U.S. Army TM 5-853</i></p>	
6.18	<p>Are fire dampers installed at all fire barriers?</p> <p>Are all dampers functional and seal well when closed?</p>	<p>All dampers (fire, smoke, outdoor air, return air, bypass) must be functional for proper protection within the building during an incident.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.19	<p>Do fire walls and fire doors maintain their integrity?</p>	<p>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.</p> <p>Reference: <i>LBNL Pub 51959</i></p>	

Section	Vulnerability Question	Guidance	Observations
6	Mechanical Systems (HVAC and CBR)		
6.20	Do elevators have recall capability and elevator emergency message capability?	<p>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.</p> <p>Reference: <i>LBNL Pub 51959</i></p>	
6.21	Is access to building information restricted?	<p>Information on building operations, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.22	Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure CBR equipment is functional?	<p>Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired.</p> <p>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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
7	Plumbing and Gas Systems		
7.1	What is the method of water distribution?	<p>Central shaft locations for piping are more vulnerable than multiple riser locations.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.2	What is the method of gas distribution? (heating, cooking, medical, process)	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.3	Is there redundancy to the main piping distribution?	<p>Looping of piping and use of section valves provide redundancies in the event sections of the system are damaged.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
7	Plumbing and Gas Systems		
7.4	<p>What is the method of heating domestic water?</p> <p>What fuel(s) is used?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.5	<p>Where are gas storage tanks located? (heating, cooking, medical, process)</p> <p>How are they piped to the distribution system? (above or below ground)</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.6	<p>Are there reserve supplies of critical gases?</p>	<p>Localized gas cylinders could be available in the event of damage to the central tank system.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8	Electrical Systems		
8.1	<p>Are there any transformers or switchgears located outside the building or accessible from the building exterior?</p> <p>Are they vulnerable to public access?</p> <p>Are they secured?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.2	<p>What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.3	<p>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?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
8	Electrical Systems		
8.4	<p>Are critical electrical systems collocated with other building systems?</p> <p>Are critical electrical systems located in areas outside of secured electrical areas?</p> <p>Is security system wiring located separately from electrical and other service systems?</p>	<p>Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.5	<p>How are electrical distribution panels serving branch circuits secured or are they in secure locations?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.6	<p>Does emergency backup power exist for all areas within the building or for critical areas only?</p> <p>How is the emergency power distributed?</p> <p>Is the emergency power system independent from the normal electrical service, particularly in critical areas?</p>	<p>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.</p> <p>Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
8.7	<p>How is the primary electrical system wiring distributed?</p> <p>Is it collocated with other major utilities?</p> <p>Is there redundancy of distribution to critical areas?</p>	<p>Central utility shafts may be subject to damage, especially if there is only one for the building.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
9	Fire Alarm Systems		
9.1	<p>Is the building fire alarm system centralized or localized?</p> <p>How are alarms made known, both locally and centrally?</p> <p>Are critical documents and control systems located in a secure yet accessible location?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.2	<p>Where are the fire alarm panels located?</p> <p>Do they allow access to unauthorized personnel?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.3	<p>Is the fire alarm system standalone or integrated with other functions such as security and environmental or building management systems?</p> <p>What is the interface?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.4	<p>Do key fire alarm system components have fire- and blast-resistant separation?</p>	<p>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.</p>	
9.5	<p>Is there redundant off-premises fire alarm reporting?</p>	<p>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.</p>	
10	Communications and IT Systems		
10.1	<p>Where is the main telephone distribution room and where is it in relation to higher-risk areas?</p> <p>Is the main telephone distribution room secure?</p>	<p>One can expect to find voice, data, signal, and alarm systems to be routed through the main telephone distribution room.</p> <p>Reference: <i>FEMA 386-7</i></p>	

Section	Vulnerability Question	Guidance	Observations
10	Communications and IT Systems		
10.2	<p>Does the telephone system have an uninterruptible power supply (UPS)?</p> <p>What is its type, power rating, and operational duration under load, and location? (battery, on-line, filtered)</p>	<p>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.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
10.3	<p>Where are communication systems wiring closets located? (voice, data, signal, alarm)</p> <p>Are they collocated with other utilities?</p> <p>Are they in secure areas?</p>	<p>Concern is to have separation distance from other utilities and higher-risk areas to avoid collateral damage.</p> <p>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.</p> <p>Reference: <i>FEMA 386-7</i></p>	
10.4	<p>How is the communications system wiring distributed? (secure chases and risers, accessible public areas)</p>	<p>The intent is to prevent tampering with the systems.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
10.5	<p>Are there redundant communications systems available?</p>	<p>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.</p> <p>A base radio communication system with antenna can be installed in stairwells, and portable sets distributed to floors.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
10.6	<p>Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure?</p> <p>Where are the secondary and/or intermediate distribution facilities and are they secure?</p>	<p>Concern is collateral damage from manmade hazards and redundancy of critical functions.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
10.7	<p>What type and where are the Wide Area Network (WAN) connections?</p>	<p>Critical facilities should have two Minimum-Points-of-Presence (MPOPs) where the telephone company's outside cable terminates inside the building. It is functionally a service entrance connection that demarcates where the telephone company's property stops and the building owner's property begins. The MPOPs should not be collocated and they should connect to different telephone company central offices so that the loss of one cable or central office does not reduce capability.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
10	Communications and IT Systems		
10.8	What are the type, power rating, and location of the uninterruptible power supply? (battery, on-line, filtered) Are the UPS also connected to emergency power?	Consider that UPS should be found at all computerized points from the main distribution facility to individual data closets and at critical personal computers/terminals. Critical LAN sections should also be on backup power. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	

Section	Vulnerability Question	Guidance	Observations
10	Communications and IT Systems		
10.12	Where is the disaster recovery / mirroring site?	A site with suitable equipment that allows continuation of operations or that mirrors (operates in parallel to) the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
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: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
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: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
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: <i>DoD UFC 4-010-01</i>	
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: <i>GSA PBS-P100</i>	

Section	Vulnerability Question	Guidance	Observations
11	Equipment Operations and Maintenance		
11.1	<p>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)</p> <p>Do updated operations and maintenance (O&M) manuals exist?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
11.2	<p>Have critical air systems been rebalanced?</p> <p>If so, when and how often?</p>	<p>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.</p> <p>Rebalancing may only occur during renovation.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
11.3	<p>Is air pressurization monitored regularly?</p>	<p>Some areas require positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation.</p> <p>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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
11.4	<p>Does the building have a policy or procedure for periodic recommissioning of major Mechanical/Electrical/Plumbing (M/E/P) systems?</p>	<p>Recommissioning involves testing and balancing of systems to ascertain their capability to perform as described.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
11.5	<p>Is there an adequate O&M program, including training of facilities management staff?</p>	<p>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.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
11.6	<p>What maintenance and service agreements exist for M/E/P systems?</p>	<p>When an in-house facility maintenance work force does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Section	Vulnerability Question	Guidance	Observations
11 Equipment Operations and Maintenance			
11.7	Are backup power systems periodically tested under load?	<p>Loading should be at or above maximum connected load to ensure available capacity and automatic sensors should be tested at least once per year.</p> <p>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.</p> <p>Reference: <i>FEMA 386-7</i></p>	
11.8	Is stairway and exit sign lighting operational?	<p>The maintenance program for stairway and exit sign lighting (all egress lighting) should ensure functioning under normal and emergency power conditions.</p> <p>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.</p> <p>Reference: <i>FEMA 386-7</i></p>	
12 Security Systems			
Perimeter Systems			
12.1	<p>Are black/white or color CCTV (closed circuit television) cameras used?</p> <p>Are they monitored and recorded 24 hours/7 days a week? By whom?</p> <p>Are they analog or digital by design?</p> <p>What are the number of fixed, wireless, and pan-tilt-zoom cameras used?</p> <p>Who are the manufacturers of the CCTV cameras?</p> <p>What is the age of the CCTV cameras in use?</p>	<p>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.</p> <p>Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras.</p> <p>Reference: <i>GSA PBS P-100</i></p>	

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
12.2	<p>Are the cameras programmed to respond automatically to perimeter building alarm events?</p> <p>Do they have built-in video motion capabilities?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.4	Are panic/duress alarm buttons or sensors used, where are they located, and are they hardwired or portable?	<p>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.</p> <p>Reference: <i>GSA PBS P-100</i></p>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.7	Who monitors the CCTV system?	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
12.8	What is the quality of video images both during the day and hours of darkness? Are infrared camera illuminators used?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>GSA PBS-P100</i>	
12.11	Is a global positioning system (GPS) used to monitor vehicles and asset movements?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
12.13	Are the cameras programmed to respond automatically to interior building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.14	What type of camera housings are used and are they designed to protect against exposure or tampering?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.15	Do the camera lenses used have the proper specifications, especially distance viewing and clarity?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.16	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.17	Are the interior camera video images of good visual and recording quality?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.18	Are the interior cameras supported by an uninterruptible power supply source, battery, or building emergency power?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.19	What are the first costs and maintenance costs associated with the interior cameras?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.20	What type of security access control system is used?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
	Are the devices used for physical security also used (integrated) with security computer networks (e.g., in place of or in combination with user ID and system passwords)?		
12.21	What type of access control transmission media is used to transmit access control system signals (same as defined for CCTV cameras)?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.22	What is the backup power supply source for the access control systems? (battery, uninterruptible power supply)	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>GSA PBS P-100</i>	
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: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
12.27	What type of interior IDS sensors are used: electromagnetic; fiber optic; active infrared-motion detector; photoelectric; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches?	Consider magnetic reed switches for interior doors and openings. Reference: <i>GSA PBS-P100</i>	
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: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
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 <i>NFPA 101, Life Safety Code</i> . Reference: <i>GSA PBS-P100</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

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

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
12.38	Are vaults or safes in the building? Where are they located?	<p>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.</p> <p>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.</p> <p>Safes and vaults may also require security sensors and equipment, depending upon the level of protection and defensive layers needed.</p> <p>Reference: <i>U.S. Army TM 5-85</i></p>	
Security System Documents			
12.39	Have security system as-built drawings been generated and are they ready for review?	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.40	Have security system design and drawing standards been developed?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.41	Are security equipment selection criteria defined?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Section	Vulnerability Question	Guidance	Observations
12	Security Systems		
12.42	What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.43	Have security system construction specification documents been prepared and standardized?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.44	Do all security system documents include current as-built drawings?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.45	Have qualifications been determined for security consultants, system designers/engineers, installation vendors, and contractors?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
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: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.47	What security systems manuals are available?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.48	What maintenance or service agreements exist for security systems?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Section	Vulnerability Question	Guidance	Observations
13	Security Master Plan		
13.1	<p>Does a written security plan exist for this site or building?</p> <p>When was the initial security plan written and last revised?</p> <p>Who is responsible for preparing and reviewing the security plan?</p>	<p>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.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
13.2	<p>Has the security plan been communicated and disseminated to key management personnel and departments?</p>	<p>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.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
13.3	<p>Has the security plan been benchmarked or compared against related organizations and operational entities?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
13.4	<p>Has the security plan ever been tested and evaluated from a benefit/cost and operational efficiency and effectiveness perspective?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
13.5	<p>Does the security plan define mission, vision, and short- and long-term security program goals and objectives?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
13.6	<p>Are threats/hazards, vulnerabilities, and risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?</p>	<p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
13.7	<p>Has a security implementation schedule been established to address recommended security solutions?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

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

Section	Vulnerability Question	Guidance	Observations
13	Security Master Plan		
13.15	<p>Are the following areas of security analysis addressed in the security master plan?</p> <p>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?</p> <p>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)</p> <p>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)</p> <p>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?</p>	<p>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.</p> <p>Reference: <i>USA TM 5-853, Security Engineering</i></p>	

***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