Security Assessment at First Entry

Vulnerabilities and Options for Consideration Library

Category	Vulnerability	Options for Consideration
Facility Information	Facility personnel are not aware of the nationwide "If You See Something, Say Something™" public awareness campaign. This program is intended to raise public awareness of indicators of terrorism and terrorism-related crime and to emphasize the importance of reporting suspicious activity to the proper authorities.	• Consult your local PSA for information about the "If You See Something, Say Something™" public awareness campaign. For more information, visit the DHS website at https://www.dhs.gov/see-something-say-something/campaign-materials.

Category	Vulnerability	Options for Consideration
First Preventers-Responders	The primary law enforcement agency has not conducted an onsite visit of the facility. Onsite visits can familiarize first responders with the facility, key personnel, site layout, and other issues that would enhance incident response.	• Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout. [1] • Establish annual onsite visits for first responders to maintain their familiarity with the facility. [1] • Develop and provide emergency responders with an offsite emergency responder booklet that includes facility floor plans and identifies utility shutoffs, outside exits, etc. [2]
First Preventers-Responders	The facility does not have interoperable communications with the primary law enforcement agency. Without interoperable communications, the facility cannot communicate with first responders in order to coordinate security and response activities.	• Collaborate with the agency on potential solutions to achieve cost-effective interoperable communications onsite. [1]
First Preventers-Responders	The primary fire response agency has not conducted an onsite visit of the facility. Onsite visits can familiarize first responders with the facility, key personnel, site layout, and other issues that would enhance incident response.	• Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout. [1] • Establish annual onsite visits for first responders to maintain their familiarity with the facility. [1]

Category	Vulnerability	Options for Consideration
First Preventers-Responders	The facility does not have interoperable communications with the primary fire response agency. Without interoperable communications, the facility cannot communicate with first responders in order to coordinate response activities.	• Collaborate with the agency on potential solutions to achieve cost-effective interoperable communications onsite. [1]
First Preventers-Responders	The primary emergency medical response agency has not conducted an onsite visit of the facility. Onsite visits can familiarize first responders with the facility, key personnel, site layout, and other issues that would enhance incident response.	• Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout. [1] • Establish annual onsite visits for first responders to maintain their familiarity with the facility. [1]
First Preventers-Responders	The facility does not have interoperable communications with the primary emergency medical response agency. Without interoperable communications, the facility cannot communicate with first responders in order to coordinate response activities.	• Collaborate with the agency on potential solutions to achieve cost-effective interoperable communications onsite. [1] • Explore the option of an interconnect system, such as a gateway that can allow communication between radio systems that are otherwise incompatible because they operate on different frequency bands or using different technologies. [3]

Category	Vulnerability	Options for Consideration
Information Sharing	The facility does not exchange information with the FBI. Information exchange with the FBI would enhance the security and resilience posture of the facility.	• Consult your local police department, sheriff's office, and/or PSA regarding opportunities to enhance information sharing with the JTTF. Information about JTTFs is also available via the FBI website, at https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces. [4]
Information Sharing	The facility does not exchange information with the ISAC for its sector. Information exchange with the ISAC would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with the appropriate ISAC. Additional information is available via the National Council of ISACs website, at https://www.nationalisacs.org. [4]
Information Sharing	The facility does not exchange information through the HSIN portal. Using the HSIN portal for information sharing would enhance the security and resilience posture of the facility.	• Consult your local PSA to become a member of the HSIN community. Information about HSIN is also available via the DHS website, at https://www.dhs.gov/homeland-security-information-network-hsin. [5]
Information Sharing	The facility does not exchange information via InfraGard. Becoming a member of InfraGard would enhance the security and resilience posture of the facility.	• Consult your local PSA about becoming a member of InfraGard. Additional information is also available via the InfraGard website, at https://www.infragard.org. [5]

Category	Vulnerability	Options for Consideration
Information Sharing	The facility does not exchange information with any federal agencies. Information exchange with federal agencies would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with federal agencies, such as the FBI and other federal law enforcement (e.g., FPS, TSA, ICE), JTTF, ATF, InfraGard, U.S. Attorney's Office ATAC, DHS, NOAA, USGS, and CDC. [4] • Consult your local police department, sheriff's office, and/or PSA regarding opportunities to enhance information sharing with federal agencies, such as the FBI and other Federal law enforcement (e.g., FPS, TSA, ICE), JTTF, ATF, InfraGard, U.S. Attorney's Office ATAC, DHS, NOAA, USGS, and CDC. [4]
Information Sharing	The facility does not exchange information with state and/or major urban area fusion centers. Information exchange fusion centers would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with state and/or major urban area fusion centers. [4] • Consult your local police department, sheriff's office, and/or PSA regarding opportunities to enhance information sharing with state and/or major urban area fusion centers. [4] • Establish a liaison with state and/or major urban area fusion centers to enhance communications, coordination, and cooperation. [4]
Information Sharing	The facility does not exchange information with the state EMA. Information exchange with the state EMA would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with the state EMA. [4] • Consult your local police department, sheriff's office, and/or PSA regarding opportunities to enhance information sharing with the state EMA. [4]
Information Sharing	The facility does not exchange information with state law enforcement. Information exchange with state law enforcement would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with state law enforcement. [4] • Establish a liaison with state law enforcement to enhance information exchange, clarify emergency response roles, track threat conditions, and support investigations. [4] • Coordinate the facility's security and emergency response plans with state law enforcement. Share critical information about the facility (e.g., floor plans, location of critical assets or areas, and notification and contact lists). [4]

Category	Vulnerability	Options for Consideration
Information Sharing	The facility does not exchange information with the local EMA. Information exchange with the local EMA would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with the local EMA. [4]
Information Sharing	The facility does not exchange information with local law enforcement. Information exchange with local law enforcement would enhance the security and resilience posture of the facility.	• Consult your local PSA regarding opportunities to enhance information sharing with local law enforcement. [4] • Establish a liaison with local law enforcement to enhance information exchange, clarify emergency response roles, track threat conditions, and support investigations. [4] • Coordinate the facility's security and emergency response plans with local law enforcement. Share critical information about the facility (e.g., floor plans, location of critical assets or areas, and notification and contact lists). [4]
Information Sharing	There is a lack of formal, consistent sharing of security and safety information with neighboring properties, adjacent tenants, or associated departments.	• Establish relationships and open dialogue including regular meetings with neighboring facilities, adjacent tenants, or associated departments to share security and safety information. [6]
Security Management	The facility does not have a designated security manager. The lack of a security manager may hinder the application of security policies, programs, or procedures.	• Consider hiring a security manager or designate an employee to act as a security manager and task that person with developing, implementing, and coordinating all security-related activities. If possible, choose an employee with previous security experience. Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [7]

Category	Vulnerability	Options for Consideration
Security Management	The facility does not have a written security plan.	• Develop a comprehensive security plan specific to the facility. The plan should address issues such as the following: protection of employees, contractors/vendors, visitors, and executives; protection of sensitive information; protection of funds; facility access control procedures; suspicious activity reporting procedures; employee termination procedures; parking; mail security; background checks; prohibited items; security force; end-of-day security checks; control and accountability of equipment (including keys); electronic security systems (including CCTV); physical security inspection programs; and employee security awareness training programs. Train personnel on the plan, and exercise the plan at least once a year. [8] • Develop a comprehensive security plan specific to the facility. The plan should address topics such as the following: physical security measures and systems, security force, access control procedures, information protection, and security awareness training. In addition, the plan should include elements such as the following: an assessment of possible security risks; a review of threats to the facility and the facility's vulnerabilities; an up-to-date point of contact roster for key personnel responsible for security and first responders; and identification of critical assets or areas. Train personnel on the plan, and exercise the plan at least once a year. [8] • Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [9]

Category	Vulnerability	Options for Consideration
Security Management	The facility does not have a written security plan. Although the facility may have documentation that addresses security policies, programs, and/or procedures, it does not have a separate, comprehensive security plan.	• Develop a comprehensive security plan specific to the facility. Train personnel on the plan, and exercise the plan at least once a year. Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [10] • Develop a comprehensive security plan specific to the facility. The plan should address issues such as the following: protection of employees, contractors/vendors, visitors, and executives; protection of sensitive information; protection of funds; facility access control procedures; suspicious activity reporting procedures; employee termination procedures; parking; mail security; background checks; prohibited items; security force; end-of-day security checks; control and accountability of equipment (including keys); electronic security systems (including CCTV); physical security inspection programs; and employee security awareness training programs. Train personnel on the plan, and exercise the plan at least once a year. [8] • Develop a comprehensive security plan specific to the facility. The plan should address topics such as the following: physical security measures and systems, security force, access control procedures, information protection, and security awareness training. In addition, the plan should include elements such as the following: an assessment of possible security risks; a review of threats to the facility and the facility's vulnerabilities; an up-to-date point of contact roster for key personnel responsible for security and first responders; and identification of critical assets or areas. Train personnel on the plan, and exercise the plan at least once a year. [8] • Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [9]
Security Management	The corporate-level security plan does not reflect facility-specific needs.	• Develop a facility-specific security plan that articulates what managers, supervisors, employee, and contractor roles and responsibilities are for protecting the facility, critical areas, and high-value equipment. [11]

Category	Vulnerability	Options for Consideration
Security Management	The facility has not coordinated the security plan with local law enforcement.	• Coordinate the security plan with local law enforcement. Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [12] • Coordinate the security plan with local law enforcement, and establish mutual-aid agreements with appropriate response agencies. Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [7] • Establish a liaison and regular communication with local law enforcement and other first responders, state and federal law enforcement and counterterrorism agencies, and industry organizations to engage in information sharing, clarify response actions, track threat conditions, and support investigations. [13] • Share critical information about the facility (e.g., floor plans, the location of critical assets or areas, notification and contact lists) with local law enforcement and emergency responders. [14] • Involve facility operators, security personnel, local police, and other government services, including local fire, emergency management, and emergency services departments at several levels in security planning. Consider involving other department leads such as marketing and communications. [15] • Conduct training and exercises with law enforcement and emergency responders to familiarize them with the facility and its security and emergency procedures. [15]

Category	Vulnerability	Options for Consideration
Security Management	The facility does not train personnel on the security plan	• Train employees to do the following: identify their responsibilities under the facility's security program; recognize connections between the security program's objectives and selected security measures; remain familiar with resources for carrying out security-related responsibilities; and be prepared for security incidents. Consult the Ready.gov website for more information on training, at http://www.ready.gov/business/implementation/training. [14] Develop a security awareness program that addresses the following topics: • Why the facility requires protection strategies [16] • What actions are required to protect specific assets and areas [16] • What employees' security responsibilities are and how they can be fulfilled [16] • How employees can report program violations [16] • How employees can identify indicators of risk or danger and how to respond appropriately [16] • Train employees on suspicious activity reporting procedures, security incident (e.g. bomb threat, active shooter) response procedures, procedures for suspicious packages, access control, and end-of-day security checks. For more information, visit the Ready.gov website at http://www.ready.gov/business/implementation/emergency. [16] • Enhance the level of employee security awareness through the distribution of a security-related newsletter, emails, and posters that address threats, concerns, training opportunities, security initiatives, and problem areas. Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [12]

Category	Vulnerability	Options for Consideration
Security Management	The facility does not exercise its security plan annually.	• Test the security plan regularly with drills and tabletop exercises to ensure that adequate resources are available to implement the plan and that all operating units can perform their responsibilities as defined in the plan. [14] • Exercise the plan at least once annually to ensure it remains applicable as changes occur at the facility. Update the plan as needed.[14] • Exercise the plan regularly with employees and other appropriate personnel (e.g., building management, tenants) to ensure that adequate resources are available to implement the plan and that all operating units can perform their responsibilities as defined in the plan. [14] • Involve first responders in exercises to familiarize them with the facility and its security plans, policies, and procedures. [14] • Consult the Ready.gov website for more information, at http://www.ready.gov/business/testing/exercises. [17]

Security Management	The facility's security plan is missing key elements.	Update the security plan to include: • An assessment of possible security risks [18] • A review of threats to, and vulnerabilities of, facility operations and activities [18] • Identification of critical assets or areas [18] • Liaison with response agencies [19] • Exercising the plan [19] • Plan maintenance (e.g., review and revision) [19] • Executive protection [18]An up-to-date point of contact roster for: • Key personnel responsible for security (e.g., the security manager or a designated representative) [18] • First responders [18]Physical Security: • Management and use of physical security systems [18] • Perimeter security [18] • Parking/delivery/standoff distance [18] • Illumination [8] • Key control program [20] • Physical security inspection program [8] Electronic security systems: • Locks and technologies [8] • CCTV system [8] • Intrusion detection or alarm system [8]Security Force: • Staffing [21] • Static Post [21] • Roving Post [21] • Equipment [21] • Training [8]Access control procedures: • Employees [22]

		• Visitors [22] • Contractors [22] • Customers [22]A security awareness training program that addresses: • Terrorist incidents [14] • Security communications policy or procedures [23] • Information protection/OPSEC [23] • Personnel security [23] • Criminal activities (e.g., break-ins) [23] • Hostage situations [23] Active shooter: • Develop a response plan and training program to provide guidance on how to respond to an active shooter. Refer to the DHS website for resources, including online training, booklets, and posters, at https://www.dhs.gov/active-shooter-preparedness. [19] • Develop an active-shooter protocol in close coordination with local first responders. • Provide initial and annual recurring active-shooter training for all personnel. • Review and exercise the active shooter plan annually with all personnel. • Designate “safe rooms” throughout the facility. Ensure each room can be locked from within and has a telephone for communications with first responders. • Provide local first responders with a copy of the facility's floor plans to enhance their response capability in an active-shooter incident. • Provide local first responders with a tour of the facility to familiarize them with its layout. Internal disturbances (e.g., workplace violence): • Develop a protocol to respond to workplace violence. Refer to the FBI Website for resources, such as the January 2011 FBI Law Enforcement Bulletin: Workplace Violence Prevention, available at https://leb.fbi.gov/articles/featured-articles/workplace-violence-prevention-readiness-and-response. • Provide training on workplace violence to all personnel at initial hire and annually thereafter. • Develop a checklist of steps to be taken when terminating an employee that includes revoking access to cyber systems, email, etc. and addresses the return of keys, access cards, uniforms, and other property. [24] • Implement a policy that deals with termination procedures for hostile employees. [24]

Category	Vulnerability	Options for Consideration
		• Refer to the FEMA Emergency Management Institute's Independent Study Program training course IS-906: Workplace Security Awareness. This free, 1-hour course provides guidance to individuals and organizations on how to improve security in the workplace and is available at http://training.fema.gov/EMIWeb/IS/IS906.asp. [23]
Security Management	The facility lacks procedures for handling suspicious packages.	• Develop procedures for handling suspicious packages. [16] • Incorporate procedures on how to handle suspicious packages into initial and annual security training programs. [16] • Implement U.S. Postal Service mail center security procedures to assess, prevent, and respond to threats such as suspicious letters and packages; bomb threats; and chemical, biological, or radiological contamination. [16] • Prominently display informational materials on suspicious package indicators in the mailroom. [16] • Refer to the Ready.gov website for information about suspicious packages and letters, at http://www.ready.gov/explosions. [25] • Ensure bomb threat checklists are accessible at all work stations where inbound calls are received. [23] • Create and use a central repository for all U.S. mail and other deliveries where packages can then be picked up or delivered to addressees in a controlled manner. See U.S. Postal Service guidelines for a mail room so that if anything suspicious does occur, it will minimally impact the overall operation of the site, if at all. Consult the DHS guidance document, Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors to inform the development of policies, procedures, and training for recognizing and handling suspicious packages. [26] • Consult the DHS guidance document, Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors, available at https://www.dhs.gov/sites/default/files/publications/Mail_Handling_Document_NonFOU0%209-27-2012.pdf, to inform the development of policies, procedures, and training for recognizing and handling suspicious packages. [26] • Train facility or organization volunteers on suspicious-package and IED recognition using local explosive-detection teams for partnership opportunities. [27]

Category	Vulnerability	Options for Consideration
Security Management	The facility does not have a mass notification system or process. During an event, no method exists to alert all participants of current threats and the appropriate responses. The lack of communication or notification may lead to increased injuries or deaths.	• Implement a mass notification process using an existing speaker / intercom system. Test and exercise the process on a routine basis. [28] • Install a mass notification system that alerts participants to an event. The best system will involve sound, illumination, and vibration so that it gets the attention of the widest range of people. Test and exercise the notification system on a routine basis. [28]
Security Management	The facility has not tested, exercised or documented its mass notification system. Using an untested system can cause confusion when used during an incident.	• Test and exercise any mass notification system on a routine basis. [28]
Security Management	The customers, employees or volunteers do not display or practice situational awareness related to security.	• Provide posters, training, briefings or similar materials on a routine basis to volunteers, employees and even customers or patrons as needed. Post signage relating to emergency entry and exit points, first aid stations, and shelter locations. Encourage the importance of reporting suspicious activity. Reinforce the significance of being alert and aware of your surroundings. [29] • Encourage employees and volunteers to become involved with security or form security teams for special events. [29]
Security Management	There is no capability or process for an employee to report a security concern.	• Establish a system for reporting security concerns. Include mechanisms for the documentation, investigation, and review of related incidents and actions taken. [16]
Security Management	The facility does not participate in any security working groups.	• Join relevant security working groups. Establish liaisons and regular communications with federal, state, local, private sector, and/or industry working groups to enhance information sharing, track threat conditions, and support investigations. [30]

Category	Vulnerability	Options for Consideration
Security Management	The facility lacks procedures for handling suspicious packages.	• Conduct background checks on all employees. [31] • Conduct initial and recurring background checks on all employees. [31] • Conduct initial and recurring background checks on all employees working in positions of trust or who are assigned to critical or sensitive areas. [31] • Require contracting companies, temporary employment agencies, and/or vendors to conduct background checks on their personnel who will work at and/or visit the facility and to make such records available for audit. [31]
Security Management	The facility does not conduct background checks on all employees.	• Conduct background checks on all employees. [31] • Conduct background checks on all employees, including temporary employees. [31] • Conduct background checks on all employees, not only employees identified as critical to facility operations. [31]
Security Management	Although the facility conducts background checks on employees, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Conduct recurring background check on employees. [31] • Conduct recurring background checks on employees as appropriate. For example, recurring background checks may be necessary for employees working in positions of trust or assigned to critical or sensitive areas. Recurring background checks may occur on an annual basis, randomly, or on special occasions (e.g., when an employee is eligible for promotion). [31]
Security Management	The facility does not conduct background checks on employee security personnel.	• Conduct background checks on security personnel. [31]
Security Management	Although the facility conducts background checks on employee security personnel, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Conduct recurring background checks on security personnel. [31]
Security Management	Background checks are not conducted on contract security personnel.	• Conduct background checks on contract security personnel. [31] • Require security contracting companies to conduct background checks on their personnel who will work at the facility and to make such records available for audit. [31]

Category	Vulnerability	Options for Consideration
Security Management	Although background checks are conducted on contact security personnel, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Ensure recurring background checks are conducted on contract security personnel. [31]
Security Management	Background checks are not conducted on contractors.	• Conduct background checks on all contractors. [31] • Conduct background checks on contractors, especially those working in positions of trust or assigned to critical or sensitive areas. [31] • Require contracting companies to conduct background checks on their personnel who will work at the facility and to make such records available for audit. [31]
Security Management	Although background checks are conducted on contactors personnel, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Ensure recurring background checks are conducted on contractors. [31] • Ensure recurring background checks are conducted on contractors as appropriate. For example, recurring background checks may be necessary for contractors working in positions of trust or assigned to critical or sensitive areas. Recurring background checks may occur on an annual basis, randomly, or on special occasions (e.g., when an contractor is eligible for reassignment). [31]
Security Management	Background checks are not conducted on vendors.	• Require vendors to conduct background checks on their personnel who will work at the facility. Obtain proof from vendors that appropriate background checks have been conducted. [31]
Security Management	Although background checks are conducted on vendors, checks are conducted only at initial hire. Recurring background checks are not conducted.	• Require vendors to conduct recurring background checks on their personnel who will work at the facility. Obtain proof from vendors that recurring background checks are conducted. [31]

Category	Vulnerability	Options for Consideration
Resilience Management - Business Continuity	The facility does not have a designated business continuity manager. The lack of a designated business continuity manager may hinder the implementation of business continuity policies, programs, or procedures.	• Appoint or nominate a person with appropriate seniority and authority to be accountable for business continuity management policy and implementation. For more information, visit the Ready.gov website. [32]
Resilience Management - Business Continuity	The facility does not have a written business continuity plan.	• Develop a comprehensive business continuity plan to be implemented in the aftermath of an incident. The business continuity plan should contain the following elements: a) defined roles and responsibilities for personnel with authority during and following an incident; b) a process for activating the response; c) details to manage the immediate consequences of a disruptive incident (with regard to the welfare of individuals; strategic, tactical, and operational response options, and prevention of further loss or unavailability of prioritized activities); d) details on how and under what circumstances the facility will communicate with employees and their relatives, key interested parties, and emergency contacts; e) how the facility will continue or recover its prioritized activities within predetermined timeframes; f) details of the facility's media response following an incident; and g) a process for standing down once the incident is over. Train personnel on the plan, and exercise the plan at least once a year. For more information, visit the Ready.gov website at http://www.ready.gov/business/implementation/continuity. [33]
Resilience Management - Business Continuity	The facility does not train personnel on the business continuity plan.	• For more information, visit the Ready.gov website at http://www.ready.gov/business/implementation/training.
Resilience Management - Business Continuity	The facility trains some, but not all, personnel on the business continuity plan.	• Train all personnel on the business continuity plan annually. Document the completion of training. [34] • Provide training to the business continuity team on the roles and responsibilities as defined in the business continuity plan. Provide additional training for leaders including incident management. [35] • For more information, visit the Ready.gov website at http://www.ready.gov/business/implementation/training.

Category	Vulnerability	Options for Consideration
Resilience Management - Business Continuity	The facility does not exercise its business continuity plan annually.	• Evaluate the business continuity plan through annual exercises. Ensure exercises are designed to accomplish the following: 1) Identify planning and procedural deficiencies; 2) Test or validate recently changed procedures or plans; 3) Clarify roles and responsibilities; 4) Obtain participant feedback and recommendations for program improvement; 5) Measure improvement compared to performance objectives; 6) Improve coordination between internal and external teams, organizations, and entities; 7) Validate training and education; and 8) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective business continuity and recovery. [36]
Resilience Management - Business Continuity	The facility does not have an alternate site for continuity of business when the primary location is not accessible.	• Establish an alternate site to continue business when the primary location is not accessible. Ensure there is sufficient distance between the alternate site and the facility so they are not likely to be affected by the same incident. Identify the location of the alternate site in the business continuity plan and define who should report to the site and under what conditions. [37]
Resilience Management - Emergency Action Plan	The facility does not have a written emergency operation/emergency action plan.	• Develop a comprehensive emergency operation/emergency action plan specific to the facility. The emergency operation/action plan should assign responsibilities for carrying out specific actions to protect people (including those with special needs), property, operations, and the environment in an emergency, and to provide incident stabilization. Train personnel on the plan, and exercise the plan at least once a year. For more information, visit the Ready.gov website at http://www.ready.gov/business/implementation/emergency, and consult Developing and Maintaining Emergency Operations Plans, available at https://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf. [38]
Resilience Management - Emergency Action Plan	The facility has not coordinated the emergency operation/emergency action plan with emergency responders.	• Coordinate the emergency operation/emergency action plan with first responders. Establish MOUs/MOAs as necessary. [39]
Resilience Management - Emergency Action Plan	The facility does not train personnel on the emergency operation/emergency action plan.	• Train all personnel on the emergency operation/emergency action plan at least annually. For more information, visit the Ready.gov website at http://www.ready.gov/business/implementation/training. [40]

Category	Vulnerability	Options for Consideration
Resilience Management - Emergency Action Plan	The facility does not train volunteers, ushers, and members of the congregation or organization on emergency operation or emergency response.	• Train volunteer congregants/staff in basic life-saving procedures, such as CPR/First Aid, and Stop-the-Bleed. Ensure that AEDs, first aid kits, and Stop-the-Bleed kits are easily accessible. [41]
Resilience Management - Emergency Action Plan	The facility does not exercise its emergency operation/emergency action plan annually.	• Conduct regular drills and exercises to validate the emergency operation/emergency action plan and to evaluate the ability of personnel to carry out their assigned roles and responsibilities. For more information, visit the Ready.gov website at http://www.ready.gov/business/testing/exercises. [42] • Consult the Homeland Security Exercise and Evaluation Program website, at https://www.fema.gov/media-library/assets/documents/32326, for a set of fundamental principles that frame a common approach to exercises, among other helpful resources. [43]
Resilience Management - Emergency Action Plan	The facility has not designated or identified safe rooms for use during events where shelter-in-place, hide, or lockdown are appropriate. The use of the safe room may be in response to an active-shooter event.	• Establish emergency escape procedures and route assignments (e.g., floor plans, safe areas), including where to evacuate and how to evacuate when the primary evacuation routes are unusable. [44] • Ensure that plans clearly explain shelter-in-place and lockdown procedures, including the differences between the two. [44] • Designate sheltering sites throughout the facility. Optimal locations have ballistic protection known as “cover” which includes thick walls made of steel, cinder block, or brick and mortar; solid doors with locks; and areas with minimal glass and interior windows. [44] • Stock sheltering sites with accessible first aid and emergency kits designed for hemorrhage control, communication devices, and telephones and/or duress alarms. [44] • Ensure that all sheltering sites and evacuation routes are accessible to persons with disabilities. [44]

Category	Vulnerability	Options for Consideration
Security Force	The facility does not have a security force. The lack of an adequately sized, well-trained, and well-equipped security force limits a facility's ability to respond to security incidents and/or emergencies.	• Develop a comprehensive security plan specific to the facility. Train personnel on the plan, and exercise the plan at least once a year. Consult Facility Security Plan: An Interagency Security Committee Guide for more information. [45] • Ensure that the size of the security force allows for adequate staffing of static posts and roving patrols. [46] • Ensure that the security force has the equipment necessary to meet the requirements established by security management (e.g., uniforms, communications, personal protective equipment). [47] • Ensure that the security force receives adequate, continuous training on topics such as emergency response, weapons and self-defense, standard operating procedures, and screening and access. [48] • Provide the security force with comprehensive post orders and a dedicated command and control/operation center. [48] • Create a surge capacity plan to augment the security force during special circumstances or elevate threats. [49]
Security Force	The facility does not have a security force. Employees perform security-related duties such as patrols and security checks. The lack of an adequately sized, well-trained, and well-equipped security force limits a facility's ability to respond to security incidents and/or emergencies.	• Explore the feasibility of establishing or contracting a security force to actively protect assets, property, and employees, and to rapidly respond to security incidents and/or emergencies. Depending on state and local regulations, security personnel may be subject to registration, licensing, certification, specific training, and other requirements. [50] • Ensure that the size of the security force allows for adequate staffing of static posts and roving patrols. [46] • Ensure that the security force has the equipment necessary to meet the requirements established by security management (e.g., uniforms, communications, personal protective equipment). [47] • Ensure that the security force receives adequate, continuous training on topics such as emergency response, weapons and self-defense, standard operating procedures, and screening and access. [48] • Provide the security force with comprehensive post orders and a dedicated command and control/operation center. [51] • Create a surge capacity plan to augment the security force during special circumstances or elevated threats. [49]

Category	Vulnerability	Options for Consideration
Security Force	The facility has no security team or threat assessment team to identify potential threats or respond to security incidents. The lack of a security team may allow potential threats to go unnoticed and leave the facility without the ability to respond to security incidents.	• Establish a security or threat assessment team that can identify potential threats and respond to security incidents at the facility. [28] • Provide the security and threat assessment teams training that include basic security principles, threat indicators, and response to natural and intentional threats. [52]
Security Force	The facility does not have a surge capacity plan to provide additional security personnel during special circumstances or elevated threats.	• Establish a surge capacity plan to augment the security force during special circumstances, for example, during special events or natural disasters, and elevated threat situations. Options may include law enforcement officers (MOA, contract, and/or off-duty) or contract security (as part of an existing contract and/or another contract). Detail in the surge capacity plan the roles, responsibilities, and chain of command for both regular and surge forces. [49]
Security Force	The facility does not have an onsite security force. The company/organization employs a security force, but security personnel are not stationed at the facility. This limits the facility's ability to rapidly respond to security incidents and/or emergencies as they occur at the facility.	• Explore the feasibility of extending the security force to provide a continuous, onsite presence at the facility to actively protect assets, property, and employees, and to rapidly respond to security incidents and/or emergencies. [45]

Category	Vulnerability	Options for Consideration
Security Force	The security force does not staff static posts at the facility's SAAs or other areas where entry control, monitoring, and/or protection is necessary (e.g., main entrance, loading dock).	• Post security personnel at assets and areas where a continuous security force presence is necessary. [45] • Provide special instructions for each post, such as duties, staffing hours, and required equipment. [53] • Establish a designated method of relief for security personnel assigned to static posts. [54]
Security Force	The security force does not have communications devices. Communications equipment is essential for the safe and efficient operation of the security force and the success of its assigned mission.	• Provide additional communications equipment to the security force, such as cell phones, duress alarms, and/or panic buttons. [47]
Security Force	The security force does not receive training on emergency response procedures for bomb threats.	• Ensure the security force receives training on emergency response procedures to bomb threats. [55] • For information about bombing prevention training available through the DHS Office of Bombing Prevention, visit https://www.dhs.gov/bombing-prevention-training. [55] • Consult with your local PSA for more information on a variety of related training and resources that are available from the DHS Office of Bombing Prevention. [55] • Consult local and state law enforcement agencies' websites that may provide information and training on emergency preparedness and response to mass casualty events, including IED attacks. [56]
Security Force	The security force does not receive training on emergency response procedures for break-ins.	• Ensure the security force receives training on emergency response procedures for break-ins. [57]

Category	Vulnerability	Options for Consideration
Security Force	The security force does not receive training on emergency response procedures for hostage/barricade situations.	• Ensure the security force receives training on emergency response procedures for hostage/barricade situations. [57]
Security Force	The security force does not receive training on emergency response procedures for fires.	• Ensure the security force receives training on emergency response procedures for fires. [57]
Security Force	The security force does not receive training on emergency response procedures in the event of a HAZMAT release.	• Ensure the security force receives training on emergency response procedures for a HAZMAT release. [57] • Review the list of FEMA training materials available at http://www.training.fema.gov. [58]
Security Force	The security force does not receive training on procedures in the event of a natural disaster.	• Ensure the security force receives training on emergency response procedures for regional natural disasters [58] • Review the list of FEMA training materials available at http://www.training.fema.gov. [58]
Security Force	The security force does not receive training on CPR/First Aid.	• Ensure the security force receives training on CPR/First Aid. [59] • Review the training materials available from the Red Cross at www.redcross.org/take-a-class. [59]
Security Force	The security force does not receive training on emergency response procedures for active shooter attacks.	• Ensure the security force receives training on how to respond to an active shooter. Refer to the DHS website for more information on active shooter response training courses, materials, and workshops available through various agencies, at https://www.dhs.gov/active-shooter-preparednes. [60] • Develop active shooter response protocols in close coordination with local first responders. [60]

Category	Vulnerability	Options for Consideration
Security Force	The security force does not receive training on IED recognition.	• For information about bombing prevention training available through the DHS Office of Bombing Prevention, visit https://www.dhs.gov/bombing-prevention-training. [61] • Consult with your local PSA for more information on a variety of related training and resources that are available from the DHS Office of Bombing Prevention. [61]
Security Force	The facility does not have comprehensive post orders for the security force, which may result in situations where security personnel do not fulfill their duties and/or perform outside the scope of their duties..	• Develop post orders that describe in detail the duties and responsibilities of the security force. After comprehensive post orders are developed, ensure that they are kept current and accessible. Comprehensive post orders may serve to express the policies of the protected enterprise, summarize required officer duties, avoid problems associated with of word-of-mouth instructions, and provide a basis for site-specific training. They are the vital link between the requirements of the facility and the ability of security personnel to effectively meet those requirements. [53]
Perimeter Security	The facility does not have a perimeter fence. The lack of perimeter fencing may allow unrestricted access to the facility and critical areas within the facility.	• Install fencing appropriate for the facility type. Determine the appropriate role of the fencing either to demarcate the boundary of the site to protect against trespassing; provide access control by channeling individuals through authorized access points; and/or to protect against unauthorized entry by providing increased access delay and more time for assessment. [62] • Consult Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430), available at a https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, for more information. [63] • Employ Crime Prevention Through Environmental Design (CPTED) principles and/or barriers (e.g., bollards, decorative flower pots, high curbs, shallow ditches) to provide enhanced penetration delay. Consult Appendix A of Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430), available at www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, and Tables 2.4 and 2.5 of Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information. [64]
Perimeter Security	Less than 100% of the facility is enclosed. The lack of fencing may allow unrestricted access to the facility.	• Install additional fencing to enclose the facility to the maximum extent possible. [65] • Explore the feasibility of improving the landscape to supplement the existing facility perimeter fence. Landscaping examples include earthen berms, low-growing shrubs, plants, or trees. Shrubs or plants with spines or thorns may be used in conjunction with the fence to provide increased penetration delay. [66]

Category	Vulnerability	Options for Consideration
Perimeter Security	The fence is not clearly marked or identified with warning signs.	• Post visible, well-placed warning signs on the fence. Signs may act as a deterrent and/or provide safety information for unauthorized personnel. Signs are usually placed on boundary fences, typically at 50-foot intervals, to indicate ownership and to warn of possible danger within. In areas where two or more languages are commonly spoken, the warning signs must use both (or more) languages. [67]
Entry Controls	The facility has limited or no access control policies/procedures for employees.	• Install access control systems and/or implement access control procedures designed to permit only authorized access, detect and prevent contraband from being brought into the facility, and provide information to security personnel to facilitate the appropriate assessment and response. Effective access control can be established through the integrated use of guards, locks, credentials, and/or screening equipment (e.g., x-ray scanners, magnetometers). [68] • Post security guards at entrances to facilitate access control procedures such as credential checks and searches. If this is not possible, integrate CCTV or other surveillance equipment to facilitate remote monitoring of access points. [69] • Implement screening operations for the facility. Available screening options include, but are not limited to, x-ray scanners, magnetometers, package searches, and physical searches. Post signage to notify potential entrants that screening is a prerequisite for entry into the facility. [70] • Issue photo ID badges to all employees. Implement a process for badge verification before employees gain access to the facility. Require badges to be displayed onsite at all times. [71]

Category	Vulnerability	Options for Consideration
Entry Controls	The facility has limited or no access control policies/procedures for visitors.	• Install access control systems and/or implement access control procedures designed to permit only authorized access, detect and prevent contraband from being brought into the facility, and provide information to security personnel to facilitate the appropriate assessment and response. Effective access control can be established through the integrated use of guards, locks, credentials, and/or screening equipment (e.g., x-ray scanners, magnetometers). [68] • Review all requests for visitor access. [72] • Evaluate the need to screen visitor requests (e.g., with local law enforcement) to identify issues before authorizing access. [72] • Maintain a list of regular visitors to the facility. [72] • Post security guards at entrances to facilitate access control procedures such as credential checks and searches. If this is not possible, integrate CCTV or other surveillance equipment to facilitate remote monitoring of access points. [69] • Implement screening operations for the facility. Available screening options include, but are not limited to, x-ray scanners, magnetometers, package searches, and physical searches. Post signage to notify potential entrants that screening is a prerequisite for entry into the facility. [70] • Limit visitor access to the facility at a level consistent with onsite safety and security requirements. [72] • Require visitors to sign in and sign out.[73] • Issue badges to visitors and require badges to be displayed at all times at the facility. Collect badges when visits are complete. [73] • Escort visitors as necessary, either at all times or only in sensitive/critical areas.

Category	Vulnerability	Options for Consideration
Entry Controls	The facility has limited or no access control policies/procedures for contractors/vendors.	• Install access control systems and/or implement access control procedures designed to permit only authorized access, detect and prevent contraband from being brought into the facility, and provide information to security personnel to facilitate the appropriate assessment and response. Effective access control can be established through the integrated use of guards, locks, credentials, and/or screening equipment (e.g., x-ray scanners, magnetometers). [68] • Maintain a list of regular contractors/vendors. [74] • Post security guards at entrances to facilitate access control procedures such as credential checks and searches. If this is not possible, integrate CCTV or other surveillance equipment to facilitate remote monitoring of access points. [69] • Implement screening operations for the facility. Available screening options include, but are not limited to, x-ray scanners, magnetometers, package searches, and physical searches. Post signage to notify potential entrants that screening is a prerequisite for entry into the facility. [70] • Limit contractor/vendor access to the facility at a level consistent with onsite safety and security requirements. [72] • Require contractors/vendors to sign in and sign out. [73] • Issue badges to contractors/vendors and require badges to be displayed at all times at the facility. Collect badges when visits are complete. [75] • Escort contractors/vendors as necessary, either at all times or only in sensitive/critical areas. [75]

Category	Vulnerability	Options for Consideration
Entry Controls	The facility has limited or no access control policies/procedures for customers/patrons/public.	• Install access control systems and/or implement access control procedures designed to permit only authorized access, detect and prevent contraband from being brought into the facility, and provide information to security personnel to facilitate the appropriate assessment and response. Effective access control can be established through the integrated use of guards, locks, credentials, and/or screening equipment (e.g., x-ray scanners, magnetometers). [68] • Limit customer/patron/public access to the facility at a level consistent with onsite safety and security requirements. [72] • Post security guards at entrances to facilitate access control procedures such as credential checks and searches. If this is not possible, integrate CCTV or other surveillance equipment to facilitate remote monitoring of access points. [69] • Implement screening operations for the facility. Available screening options include, but are not limited to, x-ray scanners, magnetometers, package searches, and physical searches. Post signage to notify potential entrants that screening is a prerequisite for entry into the facility. [70] • Install a video intercom system that would allow staff to interact with customers and visitors prior to gaining entry to the rest of the facility [76] • Train security volunteers and greeters to be on the lookout for suspicious persons and/or activity around their facilities, particularly during services and other gatherings. Report suspicious activity, persons, and vehicles immediately to local law enforcement and/or security personnel. [77] • Train the volunteers how to initiate lock-down procedures, if warranted, and how to communicate security information quickly. [78] • Place the security volunteer/greeter at or just outside the main entrance area(s) of the facility with the dual purpose of welcoming/vetting visitors and providing a watchful eye against potential threats approaching the facility. [78]

Category	Vulnerability	Options for Consideration
Entry Controls	The facility has limited or no access control procedures/policies for special events.	• Post security guards at entrances to facilitate access control procedures such as credential checks and searches on special event days. [79] • Implement screening operations for the facility. Available screening options include, but are not limited to, x-ray scanners, magnetometers, bag searches, and physical searches. Post signage to notify potential entrants that screening is a prerequisite for entry into the facility. [70] • Resources related to access controls for special events and other security-related topics are available from the Commercial Facilities Sector-Specific Agency. Resources are publicly available through the DHS website, at https://www.dhs.gov/commercial-facilities-sector. Such resources include the Check It! video which provides information to help employees conduct bag searches properly. Additional resources are available through HSIN. Consult your local PSA to become a member of the HSIN community. Information about HSIN is also available via the DHS website, at https://www.dhs.gov/homeland-security-information-network. [80]
Entry Controls	The facility does not have a badging system.	• Issue photo ID badges to all employees. Implement a process for badge verification before employees gain access to the facility. Collect employee badges from terminated personnel. [75] • Issue unique badges (e.g., color-coded) to visitors, contractors, vendors, cleaning crews, and temporary employees. Collect badges when visits are complete. [81] • Require badges to be displayed at all times at the facility. [75]
Entry Controls	Although the facility has a badging system in place, it is not strictly enforced.	• Enforce badging system requirements consistently. [82] • Require badges to be displayed at all times at the facility. [75]

Category	Vulnerability	Options for Consideration
Entry Controls	The facility lacks keycard (e.g., proximity card, swipe card) control policies and procedures. Without controls, keycards may be easily misused, and access control to the facility may be compromised.	• Establish a keycard control program that includes a database of cardholders and a system for the retrieval of keycards from terminated personnel. Regularly review the keycard database and access activity reports. [82] • Explore options to establish access levels (i.e., to sensitive or critical areas) using the keycard system. [82] • Evaluate the need for dedicated, trained security staff to continuously monitor keycard access control system alarm and event activity. [82] • Explore options (i.e., physical barriers, active monitoring by posted security personnel) to establish anti-passback controls that prevent cardholders from passing their keycards to grant access to someone else outside the secured area. [83] • Establish a 'no piggybacking' policy that requires everyone to use their own keycards for access. Explore options to enforce this policy, such as physical barriers (i.e., mantraps) and active monitoring by posted security personnel. [84]
Entry Controls	The facility does not use a proximity card access system.	• Explore procuring a badge access system that allows proximity card access into the facility. This system could be procured as part of planned facility upgrades and enhancements. [85]
Entry Controls	Although access controls are enforced at the site perimeter and/or building entrance(s), the facility has limited or no internal access controls.	• Identify sensitive/critical areas (e.g., control rooms, server rooms, mailrooms, fuel or chemical storage areas, utility service areas) that need access controls. Implement access controls (e.g., locks) for these areas as necessary. [86] • Explore options to restrict access to sensitive/critical areas using the existing keycard system. [87] • Explore options to restrict access to sensitive/critical areas using a keycard system. [87] • Conduct an internal circulation study to understand the feasibility of locking down building sections either manually or, preferably, with automated technology. [87]

Category	Vulnerability	Options for Consideration
Entry Controls	Facility personnel have unrestricted access throughout the site. Controls are not in place to restrict employee access to sensitive/critical areas (e.g., control rooms, server rooms, fuel or chemical storage areas, utility service areas) to only those with a valid need for admittance.	• Identify areas within the facility that need additional access controls. Implement controls (e.g., locks) for these areas as necessary. [88] • Explore options to establish access levels to sensitive/critical areas using the existing keycard system. [87] • Explore options to establish access levels to sensitive/critical areas using a keycard system. [87] • Post security guards at access points to sensitive/critical areas to enforce access control procedures such as credential checks and searches. If this is not possible, integrate CCTV or other surveillance equipment to facilitate remote monitoring of access points. [87]
Entry Controls	The facility has numerous extraneous access points for ingress, or has numerous access points that are unsecured.	• Evaluate the number of unsecured or unnecessary access points available for ingress, and explore ways to limit the number of access points or eliminate extraneous points of entry. [89]
Entry Controls	Main entrance doors are not locked, or existing locks are ineffective.	• Ensure effective locking mechanisms exist on doors. Keep doors locked when not actively monitored and in use. [90]
Entry Controls	The main entrance into the building allows for unrestricted access into the facility.	• Integrate a locked door that separates the foyer from access to the interior of the facility. [91] • Add a video intercom system for the receptionist to identify visitors before allowing them entry. [92] • Add a duress alarm (panic button) for the receptionist. [93]
Entry Controls	The facility lacks key control policies and procedures. Without controls, keys may be easily misused or duplicated without authorization, and access control to the facility may be compromised.	• Establish a key control program that includes a system for the retrieval of keys from terminated personnel and a formal inventory of key assignments. [94] • Ensure that keys cannot be easily duplicated. Options include patented and restricted key profiles with controlled manufacturing. [95] • Limit the use of master keys for secured sensitive or critical areas to select security personnel. [95] • Designate a key control officer to manage the key control program and conduct regular key inventories. [94]

Category	Vulnerability	Options for Consideration
Entry Controls	The facility has limited or no vehicle access control policies/procedures.	• Post security guards at vehicle entrances to facilitate access control procedures such as credential checks and searches. If this is not possible, integrate CCTV or other surveillance equipment to facilitate remote monitoring of vehicle access points. [69] • In the absence of a security force, pursue a policy in which facility employees are empowered to report any suspicious vehicles or activity in parking lots or structures. [69] • Explore the feasibility of executing searches on all vehicles entering the controlled parking area for the facility. [96] • Execute random searches on vehicles entering the controlled parking area for the facility. Evaluate the need to conduct searches on all vehicles at elevated threat levels. [96] • Positively identify all vehicles and drivers that enter the facility. Deny access to suspicious vehicles/drivers and those with improper documentation (e.g., cargo manifest). Deny access to drivers who fail to provide identification and/or submit to inspection. [97] • Maintain a database of employee vehicles. Issue permits for designated areas. [97] • Evaluate the feasibility of using centralized parking and shuttle services to keep vehicles away from critical areas. [97]

Category	Vulnerability	Options for Consideration
Parking, Delivery, Standoff	Vehicles can park within 400 feet of the facility. Access to the parking area is uncontrolled. The lack of rigorous vehicle access control procedures increases the vulnerability of the facility to a vehicle-borne attack.	• Explore options to implement vehicle access control procedures within 400 feet of the facility. Options to consider include vehicle screening and locked vehicle access points. [98] • Explore options to restrict parking within 400 feet of the facility, to minimize consequences from potential VBIEDs. [99] • Locate drop-off zones at least 400 feet from the facility. [99] • Locate visitor or general public parking at least 400 feet from the facility. [99] • Allow only permit parking by authorized individuals of inspected vehicles within 400 feet of the facility. [99] • (1) Determine the facility's susceptibility to blast. Consult Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information, especially Chapters 2 and 3: Chapter 2 discusses blast design concerns and protective measures for areas surrounding buildings. Chapter 3 discusses the nature of explosive blasts, their effects on buildings and occupants, and the concept of levels of protection. In addition, review the DHS Bomb Threat Stand-off Chart, available through the Homeland Security Digital Library, at https://www.hsdl.org/?abstract&did=4506. (2) Based on the facility's potential vulnerabilities, explore the feasibility of conducting a preliminary blast analysis using simple, commercially available building modeling and software designed to support the ability to address blast mitigation and potential VBIED threats, such as A.T.-BLAST by ARA Applied Research Associates. (3) Based on the results from the preliminary blast analysis, explore the feasibility of consulting with an engineering firm that specializes in structural fragility to procure a professional blast assessment to inform capital investments intended to protect personnel and the facility against blast. [99]

Category	Vulnerability	Options for Consideration
Parking, Delivery, Standoff	Uncontrolled parking is available adjacent to the facility, on the street.	• Explore the feasibility of installing high curbs and other measures to keep vehicles from departing the roadway in an effort to avoid security countermeasures. [100] • Explore the feasibility of restricting or eliminating parking along the curb, and/or eliminating street-side loading zones for high-risk assets. [101] • Request appropriate permits to restrict parking in curb lanes in densely populated areas to company-owned vehicles or key employee vehicles. [102] • Explore the feasibility of prohibiting street parking or enacting lane closure as a temporary measure during times of increased alert. Carefully plan such closures against elevated threats to avoid improvising with unaesthetic and disruptive measures. [100] • (1) Determine the facility's susceptibility to blast. Consult Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information, especially Chapters 2 and 3: Chapter 2 discusses blast design concerns and protective measures for areas surrounding buildings. Chapter 3 discusses the nature of explosive blasts, their effects on buildings and occupants, and the concept of levels of protection. In addition, review the DHS Bomb Threat Stand-off Chart, available through the Homeland Security Digital Library, at https://www.hsdl.org/?abstract&did=4506. (2) Based on the facility's potential vulnerabilities, explore the feasibility of conducting a preliminary blast analysis using simple, commercially available building modeling and software designed to support the ability to address blast mitigation and potential VBIED threats, such as A.T.-BLAST by ARA Applied Research Associates. (3) Based on the results from the preliminary blast analysis, explore the feasibility of consulting with an engineering firm that specializes in structural fragility to procure a professional blast assessment to inform capital investments intended to protect personnel and the facility against blast. [103]
Parking, Delivery, Standoff	Uncontrolled parking is available under the building.	**Parking within the building leaves the facility highly susceptible to accidental or intentional damage, but if parking elsewhere is not an option, apply the following restrictions:** • Permit parking only for company vehicles and employees of the building. [99] • Require proper credentials for all passengers. [99] • Conduct full vehicle inspections. [103] • Require ID checks for visitor parking. [103] • Ensure under-building parking is well-lighted and free of places of concealment and dead-end parking spaces. [104]

Category	Vulnerability	Options for Consideration
Parking, Delivery, Standoff	Uncontrolled parking is available above the building.	**Parking within the building leaves the facility highly susceptible to accidental or intentional damage, but if parking elsewhere is not an option, apply the following restrictions:** • Permit parking only for company vehicles and employees of the building. [99] • Require proper credentials for all passengers. [99] • Conduct full vehicle inspections. [99] • Require ID checks for visitor parking. [99] • Maximize visibility for surveillance into, out of, and across the parking garage. [99]
Parking, Delivery, Standoff	Parking in the uncontrolled parking area is not monitored in any way.	• Explore the feasibility of providing 24/7 CCTV monitoring for the parking area. Although CCTV coverage may need to be limited in its scope, it can still provide satisfactory coverage. [105] • Install cameras in areas such as the main entrance, at all vehicle access control points, guard booths, cashier booths, and elevator lobbies on every floor. This will ensure more than adequate security. [106] • Position the cameras to view the parking ramps and driveways as well as the intercom stations. [107] • Ensure lighting adequately illuminates activity in the parking area for viewing and videotaping. [108] • Ensure that the security force conducts roving patrols of the parking area. Routes and times for patrols should also be varied at frequent intervals to preclude establishing a routine that potential intruders may observe. [109] • Explore the feasibility of using facility employees to monitor uncontrolled parking areas. • Provide suspicious activity awareness training to facility employees, including topics related to uncontrolled parking areas. Provide options (e.g., hotline, direct phone or radio communications with security operations) for employees to report suspicious activity, potential threats, and incidents.
Parking, Delivery, Standoff	There are no procedures or policies to identify and act on unauthorized vehicles parked in the uncontrolled parking area for an extended period.	• Implement standard operating procedures to address unauthorized, suspicious, and extended-stay vehicles. Processes to consider include reporting vehicles to security and/or local law enforcement, and contracting with an area towing company for vehicle removal. [110] • Train security personnel on the standard operating procedures to address unauthorized, suspicious, and extended-stay vehicles. [110]

Barriers	The facility does not use barriers to mitigate high-speed avenues of approach. Barriers would reduce vehicle speeds and/or prevent vehicle penetration.	• Evaluate vehicle traffic patterns near the facility. Design and implement strategies to reduce vehicle speeds, improve pedestrian safety, and reduce the threat of vehicle approach velocities. [111] • Install barriers to mitigate high-speed avenues of approach, deny vehicle entry, and provide perimeter protection. Options include, but are not limited to, fixed and retractable bollards, engineered planters, heavy objects and trees, walls and ha-ha barriers, water obstacles, and Jersey barriers. [112] • Install fixed bollards, engineered planters, and/or heavy objects to mitigate high-speed avenues of approach. [113] • Install a bollard system that is well-integrated into the perimeter security design and the streetscape to minimize visual impact. Bollard height should typically not be more than 30 inches. Bollard spacing should be between 36 and 43 inches, depending on the kind of traffic expected and the needs of pedestrians and the handicapped. [113] • Install planters with considerable reinforcing and below-grade depth for effectiveness. Maintain a maximum distance of 4 feet between planters and other permanent streetscape elements, depending on the kind of traffic anticipated. Orient planters in a direction parallel to the curb or primary flow of pedestrian traffic. Do not place planter or a line of planters perpendicular to the curb. [113] • Install heavy objects that can resist vehicle penetration, such as boulders, sculptures, and trees. Such objects need varying degrees of embedment and reinforcement, depending on their weight, footprint, and height/width ratio. [113] • Explore the possibility of erecting walls, which includes retaining walls and freestanding walls, that may be constructed of concrete, concrete masonry, brick, natural stone, or other materials typically reinforced with steel. [113] • Install Jersey barriers. To be effective, Jersey barriers need to be embedded and include vertical anchorage of steel reinforcing through the barrier into the pavement. [113] • Install Jersey barriers as a temporary solution. Jersey barriers are relatively inexpensive and readily available. [113] • Explore the possibility of adding speed controls (e.g., serpentines or speed bumps) to limit vehicle speed at impact. [114] • Explore the possibility of installing active barriers, such as retractable bollards or a wedge system, to mitigate high-speed avenues of approach. Active barriers must be tended at all times by trained personnel and require regular maintenance to ensure continued operation. [115]

Category	Vulnerability	Options for Consideration
		• Explore the possibility of using CPTED principles, concepts, and strategies (e.g., water barriers, landscaping) to install barriers. Consult Appendix A of Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430), available at https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, and Tables 2.4 and 2.5 of Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf for more information. [116] • Employ temporary passive barriers (e.g., Jersey barriers) to eliminate straight-line vehicular access to the facility as needed (e.g., under special circumstances or during elevated threat situations). [117] • Use vehicles as temporary physical barriers to eliminate straight-line vehicular access to the facility during elevated threat conditions. [117]
Barriers	One or more unobstructed high-speed avenues of approach lead to significant areas and critical assets of the facility.	• Evaluate vehicle traffic patterns near the facility. Design and implement strategies to reduce vehicle speeds, improve pedestrian safety and increase standoff by installing bollards near entrances and critical assets. [118]
Barriers	The facility does not have a vehicle barrier plan or system to mitigate high speed vehicle intrusion or address heavy traffic flow during special events	• Develop a barrier plan or traffic plan that enhances safety and security. [119]
Building Envelope	Ground-floor windows do not have protective measures to mitigate the hazardous effects of flying glass during an explosive event.	• Consult Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information. [120]
Building Envelope	Outside air intakes are accessible and susceptible to the introduction of CBR agents.	• Install physical security measures, such as fencing, CCTV cameras, and motion detectors around air intakes to facilitate monitoring by security personnel. [121]

Category	Vulnerability	Options for Consideration
Electronic Security Systems - IDS	The facility does not have an interior IDS to detect attempted and successful security breaches.	• Evaluate the weakest points of entry into the facility and install IDS sensors as appropriate. Types of sensors used to detect interior intrusion include boundary penetration sensors, interior motion sensors, proximity sensors, door sensors, and window sensors. [122] • Consult Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information.
Electronic Security Systems - CCTV	The facility does not have a CCTV system. CCTV systems support surveillance of activities and events within and around a facility.	• Explore the feasibility of installing a comprehensive CCTV system onsite. Site-specific factors must be considered when selecting components that comprise a particular CCTV system. For example, the size of the system, in terms of the number of cameras needed, is the minimum number required to view all electronic security system sensor detection fields. In addition, some cameras may require artificial light sources. Finally, performance criteria and physical, environmental, and economic considerations must be factored into the component selection. [123] • Consult Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information. [124]
Electronic Security Systems - CCTV	The facility does not have a CCTV system. CCTV systems provide a rapid and cost-effective method for determining the source of intrusion or other detection alarms, if they are in place, and support surveillance of activities and events within and around a facility. In addition, a well-designed CCTV system provides a cost-effective supplement to security force patrols.	• Explore the feasibility of installing a comprehensive CCTV system onsite. [123]
Electronic Security Systems - CCTV	CCTV coverage of the facility's perimeter is limited.	• Evaluate CCTV coverage of the facility perimeter to determine if it meets the facility's security requirements. Explore options to increase coverage as necessary. [125]

Category	Vulnerability	Options for Consideration
Electronic Security Systems - CCTV	CCTV coverage of areas of concern, such as gates and entryways, is limited.	• Evaluate CCTV coverage of areas of concern to determine if it meets the facility's security requirements. Explore options to increase coverage as necessary. [125]
Electronic Security Systems - CCTV	CCTV coverage of the main vehicle entrance area is limited or non-existent.	• Explore the feasibility of adding a CCTV security camera to the facility's main vehicular entrance, positioned/angled to capture license plate information and view through a windshield for subject identification. [125]
Electronic Security Systems - CCTV	The facility does not use real-time monitoring for the CCTV system, which limits the facility to reviewing recorded material only.	• Evaluate the need for dedicated, trained security staff to monitor the CCTV system. Explore options to maximize the effectiveness of CCTV monitoring and observation, such as frequently rotating shifts for monitoring staff and limiting the number of cameras monitored by each staff member. [13]
Electronic Security Systems - CCTV	The CCTV video is not recorded; therefore, the facility cannot review footage to investigate or evaluate security incidents.	• Evaluate the need to record CCTV video, and select video recording and storage systems for the facility as appropriate. [126]
Illumination	Fences, gates, and/or parking areas are not illuminated. A lack of quality lighting can reduce observation capabilities and diminish the safety and security posture of the facility.	• Install lighting for fences, gates, and/or parking areas. Before installation, determine the appropriate type of lighting based on the overall requirements of the site and the building (e.g., continuous or standby). In addition, consider operational costs, such as life-cycle costs for energy and maintenance, when designing an appropriate lighting situation, because of their effect on project sustainability. [127]

Category	Vulnerability	Options for Consideration
Illumination	Lighting for fences, gates, and/or parking areas is uneven and dissimilar, causing glare and shadows, and resulting in inconsistent coverage, which can produce dark areas and shadows where intruders can go undetected.	• Update the lighting system to ensure illumination uniformity, so that security personnel can see ahead and to the sides with an absence of dark areas caused by shadows. Lighting should be brightest in secure areas, with the light gradually less in areas adjacent to high-illumination areas. [128]
Illumination	The backup power supply covers emergency lighting for only critical locations along fences and/or gates and/or in parking areas. The backup power supply does not cover most of the existing lights.	• Ensure that the backup power supply covers most existing lights, not only lights for critical locations. [129]

Option for Consideration References

[1] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Security Management, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[2] National Clearinghouse for Educational Facilities, 2008, Emergency Response Information for School Facilities, http://www.ncef.org/pubs/emergency_response.pdf, accessed April 3, 2018.

[3] FCC, 2008, FCC Report to Congress: Vulnerability Assessment and Feasibility of Creating a Back-Up Emergency Communications System, http://transition.fcc.gov/pshs/docs/clearinghouse/case-studies/ECS-vulnerability-assessment-report.pdf, accessed June 25, 2014.

[4] DHS, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf, accessed April 3, 2018.

[5] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf, accessed April 3, 2018.

[6] ASIS International, 2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use (ASIS SPC.1-2009), section 4.4.3, (p. 9) and section A.4.3, (p. 28), http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf, accessed April 3, 2018.

[7] DHS, 2015, Facility Security Plan: An Interagency Security Committee Guide, February, https://www.dhs.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf, accessed April 3, 2018. | Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Crisis Management, M. Knoke, Ed., Alexandria, VA: ASIS International.

[8] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc.

[9] DHS, 2015, Facility Security Plan: An Interagency Security Committee Guide, February,

https://www.dhs.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf, accessed April 3, 2018.

[10] DHS, 2015, Facility Security Plan: An Interagency Security Committee Guide, February, https://www.dhs.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf, accessed April 3, 2018. | Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc.

[11] Fennelly, L., Handbook of Loss Prevention and Crime Prevention, Burlington, MA: Elsevier Inc., P144-146.

[12] DHS, 2015, Facility Security Plan: An Interagency Security Committee Guide, February, https://www.dhs.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf, accessed April 3, 2018. | Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Security Management, M. Knoke, Ed., Alexandria, VA: ASIS International.

[13] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc.

[14] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Crisis Management, M. Knoke, Ed., Alexandria, VA: ASIS International.

[15] FEMA, 2010, 'Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101,' November, https://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf, accessed April 24, 2019.

[16] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Security Management, M. Knoke, Ed., Alexandria, VA: ASIS International.

[17] DHS, undated, 'Exercises,' http://www.ready.gov/business/testing/exercises, accessed April 3, 2018.

[18] Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International.

[19] DHS, 'Active Shooter Preparedness,' https://www.dhs.gov/active-shooter-preparedness, accessed April 3, 2018.

[20] Purpura, P., Security and Loss Prevention, 5th Edition, Waltham, MA: Elsevier Inc.

[21] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Security Officer Operation, M. Knoke, Ed., Alexandria, VA: ASIS International.

[22] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc. | Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Security Management, M. Knoke, Ed., Alexandria, VA: ASIS International.

[23] FEMA, 2013, 'IS-906: Workplace Security Awareness,' http://training.fema.gov/EMIWeb/IS/IS906.asp, accessed April 3, 2018.

[24] ASIS International, 2011, 'ASIS/SHRM WVPI.1-2011 Workplace Violence Prevention and Intervention,' https://www.shrm.org/ResourcesAndTools/tools-and-samples/toolkits/Documents/WVPI%20STD.pdf, accessed April 3, 2018.

[25] DHS, undated, 'Explosions,' http://www.ready.gov/explosions, accessed April 3, 2018.

[26] DHS, 2012, 'Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors,' https://www.dhs.gov/sites/default/files/publications/Mail_Handling_Document_NonFOUO%209-27-2012.pdf, accessed April 3, 2018.

[27] DHS, 2012, 'Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors,' https://www.dhs.gov/sites/default/files/publications/Mail_Handling_Document_NonFOUO%209-27-2012.pdf, accessed April 26, 2019.

[28] ISC, 2015, Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide, November, https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf, accessed May 24, 2019.

[29] Cybersecurity and Infrastructure Security Agency, Security of Soft Targets and Crowded Places–Resource Guide, April 2019, https://www.dhs.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf, accessed May 21, 2019.

[30] DHS, 2013, 'NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,' https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf, accessed April 3, 2018.

[31] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Investigation, M. Knoke, Ed., Alexandria, VA: ASIS International.

[32] ISO, 2012, Societal Security – Business Continuity Management Systems – Requirements (ISO 22301), https://www.iso.org/standard/50038.html, accessed April 3, 2018; section 5.2 p. 10.

[33] ISO, 2012, Societal Security – Business Continuity Management Systems – Requirements (ISO 22301), https://www.iso.org/standard/50038.html, accessed April 3, 2018; section 8.4.4, p. 18, section 8.5, p. 19.

[34] ISO, 2012, Societal Security – Business Continuity Management Systems – Requirements (ISO 22301), https://www.iso.org/standard/50038.html, accessed April 3, 2018; section 7.3, p. 13.

[35] DHS, undated, 'Training,' http://www.ready.gov/business/implementation/training, accessed April 3, 2018.

[36] NPFA, 2013, Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600), ch. 8, p. 1600-10, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed April 3, 2018.

[37] ISO, 2012, Societal Security – Business Continuity Management Systems – Requirements (ISO 22301), https://www.iso.org/standard/50038.html, accessed April 3, 2018; section 8.4.4, p. 19

[38] NPFA, 2013, Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600), section 6.8, p. 1600-9, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed April 3, 2018.

[39] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Crisis Management, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 23.

[40] ASIS International, 2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use (ASIS SPC.1-2009), section A.0, p. 19, http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf, accessed April 3, 2018. | NPFA, 2013, Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600), ch. 7, p. 1600-9 to 1600-10, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed April 3, 2018.

[41] DHS, undated, Stop the Bleed, https://www.dhs.gov/stopthebleed, accessed April 25, 2019.

[42] NPFA, 2013, Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600), ch. 8, p. 1600-10, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed April 3, 2018. | DHS, undated, 'Training,' http://www.ready.gov/business/implementation/training, accessed April 3, 2018.

[43] FEMA, 2013, 'Homeland Security Exercise and Evaluation Program,' https://www.fema.gov/media-library/assets/documents/32326, accessed April 3, 2018.

[44] DHS, 2015, Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide, https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf, accessed April 25, 2019,

[45] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 3-7, p. 9-5 to 9-7, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[46] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 3-6 to 3-7, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[47] Walsh, T.J., and R.J. Healy, 2011, Protection of Assets: Security Officer Operations, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 17.

[48] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 9-6, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[49] Fischer, R.J., and G. Green, 2004, Introduction to Security, 7th Edition, Burlington, MA: Elsevier Inc., p. 48-53

[50] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 3-7, p. 9-5 to 9-7, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018

[51] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 3-8, p. 9-6, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[52] DHS CISA, 2019, Security of Soft Targets and Crowded Places-Resource Guide, April https://www.dhs.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf, accessed May 24, 2019.

[53] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 3-8, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[54] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 9-5, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[55] DHS, undated, Counter-Improvised Explosive Device (IED) Training and Awareness, https://www.dhs.gov/bombing-prevention-training, accessed April 3, 2018.

[56] https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN

[57] ASIS , 2004, Private Security Officer Selection and Training (GDL PSO 11), Alexandria, VA: ASIS International.

[58] FEMA, Online Course Catalog, http://www.training.fema.gov, accessed April 3, 2018.

[59] American Red Cross, Our Class Programs, www.redcross.org/take-a-class, accessed April 3, 2018.

[60] DHS, 2008, Active Shooter – How to Respond, October, https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf, accessed April 3, 2018.

[61] DHS, undated, Counter-Improvised Explosive Device (IED) Training and Awareness, 'https://www.dhs.gov/bombing-prevention-training, accessed April 3, 2018.'

[62] DOD, 2013, Unified Facilities Criteria (UFC) - Security Fences and Gates (UFC 4-022-03), section 2-12, p. 26-28, October, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_03_2013.pdf, accessed April 3, 2018.

[63] FEMA, 2007, Risk Management Series - Site and Urban Design for Security (FEMA 430), https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[64] FEMA, 2011, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), section 2.3.4.4, p. 2-43 to 2-61, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018. | FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), Appendix A, p. A-1 to A-6, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[65] Garcia, M.L., 2006, Vulnerability Assessment of Physical Protection Systems, Burlington, MA: Elsevier Inc., p. 206.

[66] FEMA, 2011, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), section 2.4.6, p. 2-73 to 2-74, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018. | Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 60.

[67] FEMA, 2011, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06), section 2.4.4, p. 2-70, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[68] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc., p. 25, p. 187.

[69] Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 325.

[70] Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 264.

[71] DHS, 2011, Industry Protective Measures Report - Access Control Systems, p. 22.

[72] Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.

[73] DHS, 2011, Industry Protective Measures Report - Access Control Systems, p. 23.

[74] Purpura, P., Security and Loss Prevention, 5th Edition, Waltham, MA: Elsevier Inc., page 149

[75] DHS, 2011, Industry Protective Measures Report – Access Control Systems, p. 22.

[76] DHS, 2015, 'Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide', https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf, accessed April 24, 2019.

[77] DHS, undated, 'If you See Something, Say Something', https://www.dhs.gov/see-something-say-something/what-suspicious-activity, accessed April 25, 2019.

[78] FEMA, undated, https://www.fema.gov/faith-resources, accessed April 25, 2019.

[79] Norman, T.L., 2010 Risk Analysis and Security Countermeasure Selection, Boca Raton FL, CRC Press, Chapter 15

[80] DHS, 2017, 'Commercial Facilities Sector,' https://www.dhs.gov/commercial-facilities-sector, accessed April 3, 2018.

[81] DHS, 2011, Industry Protective Measures Report – Access Control Systems, p. 22-23.

[82] Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 262-263.

[83] Baker, P.R., D.J. Benny, The Complete Guide to Physical Security, 2nd Edition, Boca Raton, FL: Taylor & Francis Group, p. 99.

[84] Bacik, S., 2008, Building an Effective Information Security Policy Architecture, Boca Raton, FL: CRC Press, p. 138.

[85] Knoke, Michael E., 2015, Physical Security Principles (Alexandria, VA: ASIS International, p. 248).

[86] DHS, 2011, Industry Protective Measures Report – Access Control Systems, p. 21.

[87] Norman, T.L., 2010 Risk Analysis and Security Countermeasure Selection, Boca Raton FL, CRC Press, Chapter 16

[88] DHS, 2011, Industry Protective Measures Report – Access Control Systems, p. 21.

[89] DHS, 2011, Industry Protective Measures Report – Access Control Systems.

[90] DHS, 2015, 'Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide', https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf, accessed April 24, 2019

[91] Knoke, Michael E., 2015, Physical Security Principles (Alexandria, VA: ASIS International, p. 217-218).

[92] Knoke, Michael E., 2015, Physical Security Principles (Alexandria, VA: ASIS International, p. 217).

[93] Knoke, Michael E., 2015, Physical Security Principles (Alexandria, VA: ASIS International, p. 218).

[94] Fennelly, L., 2013, Effective Physical security, 4th Edition, Waltham, MA: Elsevier Inc., p. 141-142.

[95] Fennelly, L., 2013, Effective Physical security, 4th Edition, Waltham, MA: Elsevier Inc., p. 141.

[96] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 2.5, p. 2-30, section 5.5, p. 5-8 to 5-15, section 6.5, p. 6-22 to 6-23, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[97] DHS, 2011, Industry Protective Measures Report – Access Control Systems, p. 23.

[98] New York Police Department, 2009, Engineering Security: Protective Design for High Risk Buildings, ch. 5, http://www.nyc.gov/html/nypd/downloads/pdf/counterterrorism/nypd_engineeringsecurity_low_res.pdf, accessed April 3, 2018.

[99] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 5.8, p. 5-24, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[100] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 6.2.1, p. 6-5, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[101] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 2.5, p. 2-30, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[102] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 6.7.2, p. 6-26, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[103] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 5.8, p. 5-24, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessedApril 3, 2018.

[104] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 6.7.3, p. 6-29, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[105] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 5.8, p. 5-23 to 5-25, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018. | Fischer, R.J., E.P. Halibozek, and D.C. Walters, 2013, Introduction to Security, 9th Edition, Waltham, MA: Elsevier Inc., p. 206. | Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 166.

[106] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 5.8, p. 5-23 to 5-25, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018. | Fischer, R.J., E.P. Halibozek, and D.C. Walters, 2013, Introduction to Security, 9th Edition, Waltham, MA: Elsevier Inc., p. 206. | Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 141-142.

[107] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 5.8, p. 5-23 to 5-25, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018. | Fischer, R.J., E.P.

Halibozek, and D.C. Walters, 2013, Introduction to Security, 9th Edition, Waltham, MA: Elsevier Inc., p. 206.

[108] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 5.8, p. 5-25, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[109] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 9-5, http://www.fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018. | FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), Appendix A, p. A-2 to A-3, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[110] FEMA, 2007, Risk Management Series – Site and Urban Design for Security (FEMA 430), section 2.5, p. 2-30, section 3.3, p. 3-10 to 3-14, section 5.8, p. 5-23 to 5-25, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[111] FEMA, 2007, Risk Management Series – Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks (FEMA 430), section 3.5, p. 3-37, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[112] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, (FEMA 426/BIPS-06), section 2.3.4.4, p. 2-43 to 2-56, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[113] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 2.3.4.4, p. 2-43 to 2-56, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[114] FEMA, 2007, Risk Management Series – Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks (FEMA 430), Appendix A, p. A-5, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[115] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 2.3.4.4, p. 2-56 to 2-61, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[116] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings

(FEMA 426/BIPS-06), section 2.3.4.4, p. 2-43 to 2-56, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018. | FEMA, 2007, Risk Management Series – Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks (FEMA 430), Appendix A, p. A-1 to A-6, December, https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed April 3, 2018.

[117] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 1.8.3, p. 1-40, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[118] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 2.4.4, p. 2-34-35, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[119] U.S Department of Transportation, Federal Highway Administration, Managing Travel for Planned Special Events, Final Report September 2003. Chapter 6. http://ops.fhwa.dot.gov/eto_tim_pse/preparedness/pse/handbook.htm, accessed April 3, 2018.

[120] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, (FEMA 426/BIPS-06), https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[121] FEMA, 2003, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426), section 3.4, p. 3-35 to 3-44, December, https://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf, accessed April 3, 2018.

[122] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 5.5.1.2, p. 5-34 to 5-38, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[123] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 5.5.3, p. 5-44 to 5-50, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[124] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018.

[125] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc., p. 149-150.

[126] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc., p. 148-149.

[127] FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 2.4.3, p. 2-67 to 2-69, October, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed April 3, 2018. | Garcia, M.L., 2006, Vulnerability Assessment of Physical Protection Systems, Burlington, MA: Elsevier Inc., p. 136-138.

[128] Department of the Army, 2010, ATTP 3-39.32 (FM 3-19.30) – Physical Security, p. 5-5, August, http://www.fas.org/irp/doddir/army/attp3-39-32.pdf, accessed April 3, 2018.

[129] Garcia, M.L., 2008, The Design and Evaluation of Physical Protection Systems, 2nd Edition, Burlington, MA: Elsevier Inc., p. 145-147