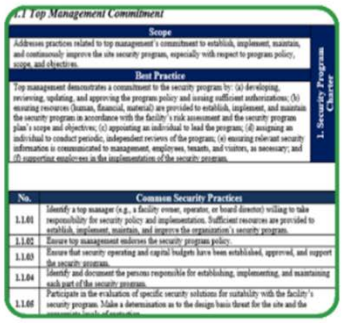
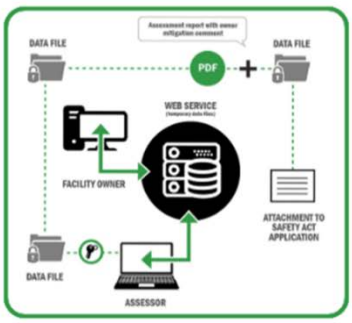
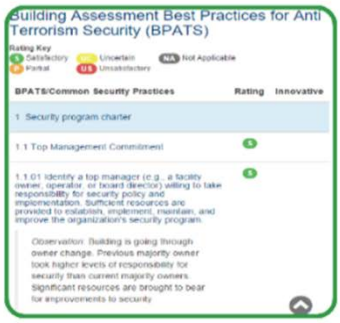
BEST PRACTICES FOR ANTI-TERRORISM SECURITY (BPATS) FOR COMMERCIAL OFFICE BUILDINGS



BPATS 1.1 Top Management Commitment



BPATS Assessment Tool Flowchart



BPATS Assessment Tool Input Screen

DHS Office of SAFETY Act Implementation

2018-08

Table of Contents

Layout of the Best Practice Listing

The following taxonomy has been established for the Best Practices for Anti-Terrorism Security (BPATS):

- At the highest level there are 7 Practice Categories used to organize the 24 BPATS. Each Practice Category contains two to five related Best Practices for Anti-Terrorism Security or BPATS. There are a total of 24 BPATS.
- Under each individual BPATS, there are three to 60 associated Common Security Practices for a total of 411 Common Security Practices.

The following figure depicts the layout of the best practice list. The Practice Category is first listed followed by the Best Practices in that category. For each Best Practice, the Title, Scope, Best Practice Statement, and Common Security Practices are enumerated.

1. Security Program Charter

1

1.1 Top Management Commitment

2

Scope: Addresses practices related to top management's commitment to establish, implement, maintain, and continuously improve the site security program, especially with respect to program policy, scope, and objectives.

3

Best Practice: Top management demonstrates a commitment to the security program by: (a) developing, reviewing, updating, and approving the program policy and issuing sufficient authorizations; (b) ensuring resources (human, financial, material) are provided to establish, implement, and maintain the security program in accordance with the facility's risk assessment and the security program plan's scope and objectives; (c) appointing an individual to lead the program; (d) assigning an individual to conduct periodic, independent reviews of the program; (e) ensuring relevant security information is communicated to management, employees, tenants, and visitors, as necessary; and (f) supporting employees in the implementation of the security program.

4

Common Security Practices	
1.1.01	A top manager is identified (e.g., a facility owner, operator, or board director) willing to take responsibility for security policy and implementation. Sufficient resources are provided to establish, implement, maintain, and improve the organization's security program.
1.1.02	Top management endorses the security program policy.
1.1.03	Security operating and capital budgets have been established, approved, and support the security program.

5

Figure 1: Layout of the BPATS Listing

1. This section indicates the practice category. There are seven categories.
2. This section indicates the title of the best practice. There are 24 best practices.
3. This statement addresses the scope of the security practices.
4. This section is the Best Practice Statement. It identifies the outcome specified by the best practice (i.e., the requirements).
5. This section identifies Common Security Practices. The security practices are suggested anti-terrorism actions, procedures, methods, or systems that execute the outcome specified by the best practice. Note that the common security practices are not all encompassing.

1. Security Program Charter

1.1 Top Management Commitment

Scope: Addresses practices related to top management's commitment to establish, implement, maintain, and continuously improve the site security program, especially with respect to program policy, scope, and objectives.

Best Practice: Top management demonstrates a commitment to the security program by: (a) developing, reviewing, updating, and approving the program policy and issuing sufficient authorizations; (b) ensuring resources (human, financial, material) are provided to establish, implement, and maintain the security program in accordance with the facility's risk assessment and the security program plan's scope and objectives; (c) appointing an individual to lead the program; (d) assigning an individual to conduct periodic, independent reviews of the program; (e) ensuring relevant security information is communicated to management, employees, tenants, and visitors, as necessary; and (f) supporting employees in the implementation of the security program.

Common Security Practices	
1.1.01	A top manager is identified (e.g., a facility owner, operator, or board director) willing to take responsibility for security policy and implementation. Sufficient resources are provided to establish, implement, maintain, and improve the organization's security program.
1.1.02	Top management endorses the security program policy.
1.1.03	Security operating and capital budgets have been established, approved, and support the security program.
1.1.04	The persons responsible for establishing, implementing, and maintaining each part of the security program are identified and documented.
1.1.05	Review and evaluate security strategies and solutions based on the design basis threat for both the facility's original design and subsequent changes and renovations/retrofits.
1.1.06	Establish security committees to share security information and engage in periodic, structured communication. Committees should include top management, security staff, tenants, long-term building occupants, and occupants of other properties with shared vulnerabilities. Security Committee procedures include names and contact information of participants.
1.1.07	Operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control.
1.1.08	Identify the primary site security officer in the site security plan. Include contact information for the officer.
1.1.09	Review incident management reports periodically (quarterly at a minimum). Amend security practices based on the results of the review.
1.1.10	Participate in security program drills and exercises.

1.2 Policy

Scope: *Addresses practices related to the site security program policy, which provides the procedural framework for making security decisions, including a strategic direction and principles of action.*

Best Practice: *The site's security program policy: (a) provides a framework for setting anti-terrorism security objectives; (b) is based on the facility's risk assessment; (c) establishes the entity's commitment to continuous improvement of the security program using measurable indicators where they are applicable; (d) is reviewed on a regular basis; (e) ensures employee adherence to security program policies; (f) is made available to authorized parties; (g) is communicated to all stakeholders; and (h) is reviewed at regular intervals (no less than annually or when significant changes occur).*

Common Security Practices	
1.2.01	The security policy complies with applicable laws, standards, and strategies based on the site's current threat environment.
1.2.02	Consider design-basis threat scenarios in setting the site's security program policy.
1.2.03	Periodically review that the security program policy, strategies, plans, and solutions are in line with the security program's requirements.
1.2.04	Consider subjecting employees that do not adhere to the security program policy to administrative (e.g., additional training or reassignment) or disciplinary action.

1.3 Scope and Objectives

Scope: *Addresses practices that relate to establishing, implementing, and maintaining the scope and objectives of the security program. Scope is defined as those aspects of site operations to which the site security program shall apply. Objectives are defined as the desired outcomes of successful implementation of the site security program.*

Best Practice: *The scope and objectives of the security program are taken into account by the site's capital investment plan and are clearly defined and documented, with regard to the following: (a) requirements of a security program for the facility; (b) roles and responsibilities of senior management, security personnel, facility operations personnel, employees, building occupants, and visitors; (c) the life safety of all occupants; (d) risk tolerance as determined by top management, with input from the security director; (e) statutory, regulatory and contractual requirements; and (f) interests of key stakeholders.*

Common Security Practices	
1.3.01	Define the mission, vision, goals, and objectives for the facility's security program.
1.3.02	Clearly define any limitations or exclusions that may apply to the security program's scope.
1.3.03	Establish a security-specific multi-year capital management plan encompassing a list of desired security enhancements. The plan should account for emerging threats and security-related systems in need of upgrades. Plans should be organized into short and long-term capital and operational resource allocation strategies.
1.3.04	Use a cost-benefit analysis and results of a risk assessment to select tailored security solutions.
1.3.05	Identify both short-term and long-term program (performance) objectives arising from risk assessments and cost/benefit analysis. Clearly indicate the desired result or end-state of response operations, defining "successful outcomes" for responders, survivors, and stakeholders. Performance objectives should include the responsible party, expected "observable and measurable" knowledge and behavior, required resources, and the method of evaluation.
1.3.06	Develop objectives consistent with the Incident Command System (ICS). Such objectives should be SMART: specific, measurable, action-oriented, realistic, and time-sensitive. (Adapted from Federal Emergency Management Agency, "Incident Command System," FEMA.gov [website], http://www.fema.gov/incident-command-system, accessed April 30, 2013.)

2. Strategic Planning

2.1 Risk Assessment

Scope: *Addresses practices that relate to conducting a risk assessment for the site and its operations.*

Best Practice: *A risk assessment that addresses threats, vulnerabilities, and consequences has been performed for the facility by a qualified individual. It is used to develop and implement the security program. The risk assessment provides a design basis threat for each threat scenario developed and prioritizes risk by considering how each asset is impacted by each threat scenario. The risk assessment is regularly reviewed (no less than annually or when significant changes occur) and is updated based on review.*

Common Security Practices	
2.1.01	Ensure objectivity of the risk assessment process by using an independent outside party to either conduct or validate the assessment.
2.1.02	Base all security program plans and procedures relating to preparedness, incident response and recovery, and continuity of operations, on the results of the facility's risk assessment.
2.1.03	Base the risk assessment for the facility on a DHS-approved risk management framework, such as the National Infrastructure Protection Plan (NIPP).
2.1.04	Quantify the risk and resilience of the facility. Reference DHS Science & Technology Building and Infrastructure Publication-04 (BIPS-04) "Integrated Rapid Visual Screening of Buildings".
2.1.05	A Risk Assessment has been conducted. Reference: DHS Science and Technology's Building and Infrastructure Protection Series (BIPS) publication BIPS-06 "Reference Manual to Mitigate Potential Terrorist Attacks Against Building".
2.1.06	Incorporate assessments of threats (likelihood), vulnerabilities (weak points), and consequences (impact) when conducting risk assessments. Use, when possible, information collected from actual prior incidents to better develop appropriate responses. Determine security countermeasures for identified risks and prioritize them relevant to their criticality and probability of occurrence.
2.1.07	The risk assessment methodology prioritizes risk by considering how each asset (e.g., people, infrastructure, systems, etc.) is impacted by each threat scenario.
2.1.08	Revise all security program plans and procedures periodically or particularly when threats, vulnerabilities, or consequences of a terrorist attack change.
2.1.09	Analyze the activities and operations in the surrounding area of the facility (e.g., airports, chemical plants, government buildings, pipelines, rail lines, transportation/subway terminals, public assembly venues, etc.) to determine if there is any potential for them to change security risks to the building. Include this analysis in all risk assessments.
2.1.10	Get input from the site's insurance broker and a cross-section of the occupants of the building when performing the risk assessment.
2.1.11	Meet with adjacent facilities regularly to discuss local and common security issues, and to share information. Include this information as part of the risk assessment.
2.1.12	The following inputs were considered in the risk assessment: the probability of an event; the magnitude and severity of the event; the time available for public warning; the probable location(s) of the event, the potential size of the affected area, the duration of consequences, and potential cascading effects.
2.1.13	Be aware of materials already in place at the building that could be leveraged for illicit purposes (e.g., flammable materials, hazardous chemicals, etc.). Include this information in the vulnerability part of the risk assessment.
2.1.14	Consider the impact on facility operations if all essential computer system resources (command, control, and financial computer systems) are disconnected from the internet and public access.

2.1 Risk Assessment	
2.1.15	Consider the type and number of visitors that are typically in the facility as part of all threat assessments.
2.1.16	Establish protective measures and mitigation actions to be set in place based on the threat condition.
2.1.17	Maintain dialogue between tenants, vendors and building management to exchange information on recently terminated employees that pose a possible security risk. Include this information in a threat assessment. Provide a special alert notification, including a photograph of the individual, if available, to all security staff.
2.1.18	Organize risk information into a format that is easily usable by the planning team.
2.1.19	Create a rating system, either qualitative (high, med, low) or quantitative (1-10) to rank incidents and help set priorities for investment. Include this information in the risk assessment.
2.1.20	Review the risk assessment periodically and, in particular, when a new asset (i.e., an addition to the facility, parking lot, or new type of revenue service) is added or when a change in condition warrants a review. Update the assessment based on the review.

2.2 Risk Awareness

Scope: *Addresses practices that relate to establishing, implementing, and maintaining situational awareness of risks to the facility*

Best Practice: *Awareness of foreseeable risk (threats, vulnerabilities, and consequences) is maintained in accordance with the security program policy, scope, and objectives. Efforts are taken to identify changes to threats, vulnerabilities, and consequences. When changes are identified, the security program is updated as necessary.*

Common Security Practices	
2.2.01	Immediately conduct a system-wide risk assessment when a change in conditions warrants it (e.g., intelligence indicates a change in threats).
2.2.02	Identify a liaison from the security staff to maintain regular communication with DHS, local law enforcement and FBI, federal and state homeland security advisors, public health organizations, and industry organizations. Regularly exchange information, threat conditions, suspicious activity, and investigative support.
2.2.03	Monitor the National Terrorism Advisory System (NTAS) and Maritime Security (MARSEC) threat levels and take appropriate precautions consistent with the risk assessment.
2.2.04	Participate in established communications network with neighboring facilities or local police and fire departments, such as CEAS (Corporate Emergency Access System). Participate in established REISAC (Real Estate Information Sharing and Analysis Center) through subscription to e-mail notifications.
2.2.05	Maintain awareness of changing security risks to the site. When addressing changing security risks, always consider the following: the impact of nearby facilities and properties (e.g., government buildings, airports, stadiums, convention centers, industrial plants, pipelines, railroads, etc.); the impact on the facility if neighboring facilities are attacked. This is particularly important if a nearby facility is attractive to terrorist activity (e.g., critical infrastructure, government, military, recreational areas, transportation, utilities, etc.); and the potential impact of identified or emerging risks to the facility.
2.2.06	Monitor nearby land use and future development plans, particularly those that are on the immediate perimeter of the site. Monitor nearby building use changes (i.e. office to school facility) or change in tenant profile for potential threat either in building or nearby.
2.2.07	Maintain up-to-date contact information for internal stakeholders (e.g., employees, tenants, etc.) and external stakeholders (e.g., first responders, government officials, etc.) for potential outreach and networking and sharing of information.
2.2.08	Deter or prevent the use of photography of sensitive areas and closely monitor photography in public areas (i.e., tourist photogenic areas) in accordance with site risk tolerance.
2.2.9	Establish a Common Operating Picture by integrating data from security system elements (e.g., access control, CCTV, security alarms, fire/life safety systems, HVAC systems, Chemical Biological Nuclear Radiological and Explosive (CBRNE) systems, etc.).

2.3 Incident Preparedness

Scope: *Addresses practices that relate to developing and documenting site security plans that address preparing for, mitigating and deterring, responding to, and recovering from an act of terrorism.*

Best Practice: *Plans have been established, implemented, and maintained to support prevention, mitigation, response, recovery, business continuity operations, and drills and exercises in connection with a terrorist attack. These plans are consistent with the findings of the risk assessment. The plans are documented and include documented agreements with first responders. The plans are developed by qualified individuals.*

	Common Security Practices
2.3.01	Use site risk assessments to develop and maintain incident management plans and response procedures.
2.3.02	Include input from a cross section of employees, building tenants, vendors, long-term contractors, and security personnel when developing security plans. Invite law enforcement and first responders to participate.
2.3.03	Identify potential incident commanders either by position type or name. Require designated incident commanders to become familiar with the NIMS.
2.3.04	Interdependencies and resource availability are considered during formulations of plans and procedures.
2.3.05	Establish, implement, and maintain policies and procedures to activate an emergency operations command center(s) and initiate the incident command system.
2.3.06	Establish, implement, and maintain incident command procedures that include a unified command plan with appropriate stakeholders (e.g., local law enforcement, emergency responders, or other government agencies). Appropriate local law enforcement personnel and emergency responders should know the names of and have contact information for the organization's security team and the appropriate members of the incident command structure.
2.3.07	Establish, implement, and maintain a process for the reporting of suspicious activities, objects, and occurrences to appropriate security, building management, or appropriate authorities. Ensure procedures exist for questioning people acting suspiciously or violating security regulations, and denying access to those persons.
2.3.08	Establish, implement, and maintain procedures for periodic inspections of protected and restricted areas in the facility, including lockers and storage areas, at higher threat or other conditions as specified in the facility's risk assessment.
2.3.09	Establish, implement, and maintain a response plan. Address lifesaving and mitigation-of-impact procedures, which should be taken immediately after an incident (e.g., restricting entrance to the impacted areas, protecting undamaged property, preventing tampering of the scene, etc.). Model the plan on the National Incident Management System (NIMS). Include directions for restricting entrance to the impacted areas that will protect the life of survivors and responders, protect undamaged property, prevent tampering of the scene, and in general, prevent further negative impacts.
2.3.10	Establish, implement, and maintain an occupant emergency plan that directs occupants on how to react to emergency situations.
2.3.11	Establish, implement, and maintain a communication and notification plan that covers voice, data, and video transfer of information related to safety and security. Provide a simple and straightforward means for people to send and receive information regarding a potential threat or an emergency.
2.3.12	Establish, implement, and maintain a liaison with First Responders concerning decontamination plans (e.g., for chemical, biological, radiation, and nuclear [CBRN] materials) for the building, taking into account neighboring infrastructure and facilities. Ensure the buildings Incident response plans do not conflict with the plans of the First Responders.
2.3.13	Establish, implement, and maintain emergency procedures that include contingencies for the loss of power, heating, cooling, water and sewage and other vital utilities.

2.3 Incident Preparedness	
2.3.14	Establish, implement, and maintain an evacuation plan for the facility. Ensure plans address the needs of special needs staff and occupants (e.g., persons with hearing or visual impairments, persons with poor reading skills, or non-English speakers). Coordinate site evacuation plans with commercial tenant plans and all neighboring facilities; meet annually to exercise and update plans.
2.3.15	Establish, implement, and maintain procedures for shelter-in-place or safe room situations. Indicate which emergency situations (e.g., active shooter) necessitate sheltering-in-place or moving to safe room locations.
2.3.16	Establish, implement, and maintain written procedures for the HVAC (heating, ventilation, and air-conditioning) system control (e.g., emergency shutdown, set for 100 percent recirculated air, etc.).
2.3.17	Establish, implement, and maintain a recovery plan. Address procedures for restoring mission critical functions once incident response has been completed. Consider including actions such as: reopening undamaged areas, reduction in services, and activation of memoranda of understanding.
2.3.18	Establish, implement, and maintain a plan for post-incident employee counseling (incident stress management, psychological services, and family assistance).
2.3.19	Establish, implement, and maintain contingency plans to provide for the welfare of employees and their families, such as assistance with overnight shelter and food.
2.3.20	Establish, implement, and maintain organizational plans that address security procurement, workplace violence, prohibited items and substances, and key control.
2.3.21	Identify primary and alternate evacuation routes and assembly locations (muster points).
2.3.22	Emergency management and site security personnel and other authorized users have immediate access to all security and emergency response plans (e.g., emergency plans, emergency instructions, and building plans, the facility security plan, and contact and communication information).
2.3.23	Set in place emergency response memorandums of agreement or mutual aid agreements.
2.3.24	Document areas within the building with uninterruptible power supply (UPS) and batteries. Identify their locations and make sure their locations are known by appropriate response personnel.
2.3.25	Document locations in the facility where chemicals and other hazardous materials may be found, particularly in chemical storage areas. Mark the entrances to these locations with clear signage. Share this information with appropriate response personnel.
2.3.26	Document the names and contact information of appropriate law enforcement personnel and emergency responders. When feasible, security personnel and crisis management leaders should be familiar with local law enforcement and emergency response personnel and procedures.
2.3.27	Coordinate with local agencies the emergency access lanes for fire, police, and emergency medical services (EMS) personnel. In addition, coordinate the location of areas where appropriate response personnel can establish incident command posts.
2.3.28	Include and maintain in incident plans the contact information and pertinent information for disaster recovery services.
2.3.29	Coordinate with local agencies the emergency access lanes for fire, police, and emergency medical services (EMS) personnel. In addition, coordinate the location of areas where appropriate response personnel can establish incident command posts.
2.3.30	Plans include post-event procedures for recording vital information about an incident, actions taken, decisions made, and lessons learned. Include in incident management procedures a requirement to have a post-event debrief to identify lessons learned.
2.3.31	Invite municipal entities (e.g., fire, local law enforcement) to review and assess building security plans and procedures.
2.3.32	Ensure all retail occupants are familiar with applicable site security procedures.

2.3 Incident Preparedness	
2.3.33	Each facility shall have an armed attacker (active threat armed with any type of weapon (e.g., firearm, knife, explosives, etc.)) preparedness plan, which is to be updated at a minimum every two years, or as needed based upon events/incidents. At a minimum, a plan should comprise the following elements: a. Security Assessments; b. Preparedness; c. Communication; d. Incident Plan (i.e., actions to take during an incident); e. Training and Exercises; f. Post Incident Recovery for Employees and Operations of the property. Note: the plan need not be a standalone document. (Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide, Nov. 2015.)
2.3.34	Encourage retail occupants to develop a business continuity plan that is consistent with facility security plans.
2.3.35	Document the time of the last revision for each security plan used in the site security program.
2.3.36	Establish an armed attack exercise program. Identify the best training approach for different facility occupants (general public, tenants, facility management, security staff). Conduct different types of exercises according to a group's training needs. (For example: tenants would benefit from participation in discussion-based exercises, such as seminars, or armed attack drills. Employees, facility management and security would benefit from Table Top Exercises and hands-on scenario-based training.) Extend exercise participation opportunities to the external emergency responders likely to support the facility in an active armed attack situation.
2.3.37	Facility Management (or as coordinated, tenant management) shall provide training, materials, and/or awareness discussions to inform building/facility employees of active shooter preparedness plans as they are updated. Building/facility employees should be aware of the Federally-endorsed run-hide-fight concept. Building/facility employees should be informed of the importance of having a personal plan. New building/facility employees should be given active armed attacker preparedness training during the initial onboarding period.
2.3.38	Facility management shall collaborate with the facility security provider, on-site law enforcement agencies (if applicable), and first responder agencies likely to address an armed attack situation to confirm local response protocols, identification of potential operational issues that might be encountered or require coordination.

2.4 Incident Response and Recovery

Scope: *Addresses practices and procedures that relate to responding and recovering from an act of terrorism.*

Best Practice: *Appropriate procedures are in place to enable: (a) response for life safety and damage mitigation and (b) resilient recovery. Specific persons (e.g., area captain, marshal, warden, etc.) have been designated, trained, and resourced to conduct such operations, as necessary. Key personnel are cross-trained and procedures are rehearsed. Appropriate liaisons have been established with first responders. Procedures are based on the facility's risk assessment.*

Common Security Practices	
2.4.01	Identify potential incident commanders either by position type or name. Require designated incident commanders to become familiar with the NIMS.
2.4.02	Designate staff to serve on an emergency response team. Design the team such that it can be scaled to fit the emergency situation as described in the NIMS.
2.4.03	Maintain and have readily available at the facility a list of employees, tenants, vendors, contractors, and other non-visitor occupants. Ensure the list includes emergency contact information. Keep this list as current as possible always considering the number of facility occupants.
2.4.04	Inventory emergency equipment and supplies periodically to verify that needed quantities (per risk level) are adequately stocked, available, and within any applicable expiration date.
2.4.05	Provide in advance a list of special needs people to local first responders (fire and police).
2.4.06	Get input from local EMS on how to handle medical emergencies in the facility, including advice on where to set up first aid and triage stations and transport sites.
2.4.07	Plan and test liaison with First Responders and have the capability to share information and data (video feeds) at the Security Operations Center, or facility command center, with first responders and other agencies and entities during emergency response and recovery operations.
2.4.08	Identify a floor captain or marshal who is responsible for each floor or tenant of the site (whichever is more applicable). The captain or marshal is responsible for implementing each floor's or tenant's appropriate emergency plan, and ensuring that it is carried out properly. In the case of evacuations, check for stay-behinds.
2.4.09	When necessary, require evacuation of all occupants of the facility without specific emergency related duties.
2.4.10	Locate and address the needs of people who require special attention during a disaster (e.g., the disabled, people with poor reading skills, non-English speakers, etc.).
2.4.11	Increase on duty security staff during heightened threat conditions or in response to an incident. Account for additional security staff requirements if reinforcements or relief personnel are needed.
2.4.12	Locate muster stations in low traffic and fireproof areas near stairwells or freight elevators.
2.4.13	Recall elevators to the ground floor in the event of an emergency. Use freight elevators for responder staging or evacuation.
2.4.14	If necessary, control elevators remotely from the command center during an emergency.
2.4.15	In incident plans, comply with local code for mandatory evacuation due to fire from the affected floor and floors above and below per local code.
2.4.16	Establish incident response procedures for a kidnapping incident. Up to the limits of the security officer's authority, immediately lockdown the site in the event of a kidnapping and liaison with responding police.
2.4.17	Inspect public areas in the event of a general bomb threat. Absent positive target identification (PTI) indicators or other credible information, an evacuation may not be appropriate. Evacuate and search any area affected by a specific threat.

2.4 Incident Response and Recovery	
2.4.18	Predetermine who should approach illegally parked vehicles and provide training for those persons to best protect themselves and the public in this situation.

2.5 Continuity of Operations	
Scope: *Addresses practices that relate to ensuring the availability of the site's designated critical functions before, during, and after a terrorist incident.*	
Best Practice: *Appropriate procedures are in place or resources are available to ensure the functionality of critical activities of the security program.*	
Common Security Practices	
2.5.01	Solicit input from the all tenant organizations as to their business continuity requirements.
2.5.02	Establish, implement, maintain, and exercise COOP plans for critical incident management functions of the facility.
2.5.03	Identify alternate worksite(s), if needed, to ensure continuity of operational activities.
2.5.04	Designate an alternate or back up site for continuing critical activities during an incident.
2.5.05	Create mutual aid and resource sharing programs and agreements with neighboring buildings.
2.5.06	Conduct a business impact assessment that will help to determine the consequences if operations are disrupted.
2.5.07	Identify the maximum time between the last backup of critical information and disruption that could eliminate unrecoverable data. Develop procedures to address this potential vulnerability.
2.5.08	Identify maximum allowable recovery times for critical functions (e.g., restoration of power).
2.5.09	Create a security culture where all staff knows that backup personnel are designated to execute emergency functions if primary personnel are unavailable or incapacitated.

3. Administrative Controls

3.1 People Surety

Scope: *Addresses practices that relate to ensuring: (a) the quality, competence, and suitability of site security personnel, and (b) the ability of all relevant security and nonsecurity personnel (including staff, tenants, and certain visitors) to implement the security program, as appropriate.*

Best Practice: *Security personnel are qualified and pre-screened (background checks) in accordance with applicable legal requirements and commensurate with the risks identified for the facility. Measures are in place to attract and retain high-performing personnel. Other facility personnel (i.e., employees, vendors, contractors, and site tenants) are trained to implement the security program, as appropriate.*

Common Security Practices	
3.1.01	Screen all potential security staff to check the applicant's identity, employment history, criminal history, financial history, and overseas activity.
3.1.02	All security staff is appropriately licensed.
3.1.03	Create a set of minimum qualifications (knowledge, skills, and abilities) for hiring security staff (e.g., licensing, education requirements, knowledge and application of security practices, skill with security equipment, ability to work independently and as part of a team, ability to communicate, etc.). Consider giving preference to applicants with a college degree, relevant professional certifications, or with a law enforcement background. Ensure factors are consistent with legal requirements.
3.1.04	Create a list of disqualifying factors that can be used to reject an individual for employment. Ensure factors are consistent with legal requirements.
3.1.05	Where allowed by law, collect a biometric, typically fingerprints, from security staff employees as a condition of employment.
3.1.06	Consider hiring a qualified training coordinator that oversees employee security training needs.
Security Staff – Training	
3.1.07	Security staff training meets all jurisdictional training requirements. Consider requiring additional training requirements per quarter that are tailored for the site and include site-specific scenario reviews.
3.1.08	Create and maintain a training record for each security staff member. Regularly monitor and track the training record.
3.1.09	Provide specialized training to security personnel based on their position requirements.
3.1.10	Ensure all security staff training (including refresher training) is tailored to the particular facility (e.g., building specific security policies and procedures, workplace violence, crime prevention measures, suspicious packages, reporting security incidents, proper reporting and response to fires and other emergencies, operational security measures, and appropriate response to incidents per the facility security plan).
3.1.11	Consider rewarding members of security staff who complete optional training (e.g., online training modules).
3.1.12	Train security staff on the procedures and operation of all screening equipment.
3.1.13	Train staff to implement public awareness programs such as DHS's "If You See Something, Say Something;" campaign.
3.1.14	Train security staff to identify and question suspicious persons and how to handle unattended, left-behind packages.
3.1.15	Train security staff in first aid, cardiopulmonary resuscitation (CPR), and in the use of external defibrillators.
3.1.16	Train security staff on the location and use of manual fire-pull stations, fire extinguishers, and stairwell exits on each floor.

3.1 People Surety	
3.1.17	Train security staff on the safe approach to illegally parked vehicles.
3.1.18	Train security staff to implement response plans, specifically their individual roles and responsibilities. Give a copy of the facility's emergency plans and instructions to all new facility employees, preferably at an employee orientation session. Training should include information on the specific protective measures that the facility will implement during an emergency.
3.1.19	Train security staff on how to shut off utility services, when appropriate (e.g., emergencies).
3.1.20	Train security staff how to recognize official law enforcement uniform and identification badges.
3.1.21	Train access control staff in behavioral profiling and identification badge recognition.
3.1.22	Offer refresher training for security staff on current principles, practices, and trends in technology.
Nonsecurity Staff and Contractors – Hiring, Background, and Qualifications	
3.1.23	Perform background checks on new frontline operations and maintenance employees, as well as employees and contractors with access to sensitive security information and security critical facilities and systems.
Nonsecurity Staff and Contractors – Training	
3.1.24	Give a copy of emergency plans and instructions, particularly the evacuation plan, to all new employees preferably at an employee orientation session.
3.1.25	Provide security training on current security matters to top facility managers, including but not limited to, corporate level executives, general managers, and operations managers.
3.1.26	Train nonsecurity staff to implement response plans, specifically their individual roles and responsibilities (when applicable). Give a copy of facility emergency instructions to all new facility employees, preferably at an employee orientation session.
3.1.27	Train facility staff, including part-time, adjunct, logistics, and contract employees, to identify suspicious people, objects, and activities.
3.1.28	Instruct staff to secure sensitive material (e.g., not leaving sensitive items lying on desktops, logging off computers when not present, etc.).
3.1.29	Train building tenants in the proper use of available emergency equipment, such as fire extinguishers, heart defibrillator, etc. Instruct those not trained not to operate emergency equipment.
3.1.30	Train all tenants on the use and location of manual fire-pull stations, fire extinguishers, and stairwell exits on each floor.

3.2 Identification and Verification

Scope: *Addresses practices that relate to the identification, verification, and appropriate credentialing of persons and objects on site, as necessary.*

Best Practice: *The identification system clearly identifies and verifies authorized personnel, guests, vehicles, and deliveries, and mitigates system abuse through control measures.*

Common Security Practices	
3.2.01	The security office exercises sole control over the facility's identification and verification system (e.g., issuing and revoking identification badges, etc.).
3.2.02	Issue identification badges containing photographs to building employees, tenants, contractors, cleaning crews, vendors, and temporary employees. Require that all identification badges be displayed at all times and verified to gain access to the building.
3.2.03	Indicate the following on the identification badge: areas of access (tenant space, utility and mechanical areas, etc.) and purpose of activity on the premises (e.g., organization name, security, maintenance, etc.).
3.2.04	Identification badges are designed to be easily identifiable (e.g., color, shape, etc.).
3.2.05	Implement increased security controls (e.g., a PIN [personal identification number], biometric, etc.) to identification badges for access to sensitive or critical areas of the facility. These areas may include: utility connections, loading docks, telecommunications and IT equipment, emergency power supplies, child-care play yards, hazardous-materials storage, HVAC, and other designated critical locations.
3.2.06	Issue new identification badges to staff or tenants that dramatically change their appearance.
3.2.07	Personnel identification is worn in a visible location.
3.2.08	Create and maintain a record of identification badges issued.
3.2.09	Periodically generate a list of all personnel that have been issued identification badges. Require that all tenants notify security immediately when an employee is fired. Revoke access privileges for fired employees and, if necessary, place them on a Do Not Admit list.
3.2.10	Visitor log has the following information: name, time, organization visited, and name of person visited and purpose of visit.
3.2.11	Require requests for temporary and replacement identification badges to be made in writing, particularly the media; persons designated to pick up identification badges must do so in person using photo identification.
3.2.12	Establish, implement, and maintain procedures for reporting, replacing, and immediately deactivating lost or stolen identification badges. Require departing individuals to surrender their identification badges promptly. Ensure procedures are in place to identify employees that lose their badges.
3.2.13	Employees are encouraged to question unusual or unrecognized people in or attempting to enter areas where access is restricted.
3.2.14	Establish through training a security practice where employees do not allow anyone else to enter a controlled area at the same time without using their own credentials; this is often referred to as "piggybacking." Include instructions to this end in plans and in training sessions.
3.2.15	As necessary, ensure security guards verify the entrant's identity (e.g., matching face to photo identification). It is preferable that the guard validate the authenticity of the identification presented (e.g., physical inspection of identification).
3.2.16	Require preclearance of visitors prior to their arrival at the facility.
3.2.17	Require visitors to sign in and sign out of the site.
3.2.18	Implement an electronic access tracking system that logs entry into and exit from critical areas.

3.2 Identification and Verification	
3.2.19	Require tenants to pre-register contractors with the site security office. If not pre-registered, confirm the contractor's identity and verify appointment with the tenant prior to granting access.
3.2.20	Escort is required for all individuals (e.g., visitors, cleaning crews, delivery personnel, maintenance workers, etc.) who do not have the appropriate security clearance to be in sensitive or critical areas. Escorts should be appropriately cleared and remain with the individual.
3.2.21	Some members of the security staff wear uniforms. Plain clothed security staff are used as appropriate (e.g., to monitor crowded areas). Uniforms should convey professionalism (e.g., slacks, dress shirt, tie (for men), blazer, or in some instances, a business suit). Require uniform vendors to verify the identity of individuals seeking to purchase uniform articles.
3.2.22	All deliveries are registered with mail room or loading dock; verify registration prior to accepting deliveries. Consider holding courier's identification until delivery is complete.
3.2.23	Issue and keep a record of parking permits, including identifying information for employee-owned vehicles.
3.2.24	Vehicle identification information is collected for all vehicles authorized to park on site.
3.2.25	Enforce use of official parking permits on vehicles using segregated parking areas (e.g., employee, long-term lots). Remove non-registered or illegally parked vehicles.

3.3 Information Security

Scope: *Addresses practices that relate to the protection of sensitive intellectual property kept on site. Excludes cybersecurity.*

Best Practice: *Sensitive information including site security, company, and personnel information is protected from unauthorized access or tampering.*

	Common Security Practices
3.3.01	Establish, implement, and maintain procedures to identify, store, and control vital records (e.g., information and documents on building operations, schematics, procedures, plans, specifications, etc.). Make these available only to authorized personnel.
3.3.02	Restrict access to all security planning information. Make this available only to authorized personnel. Encrypt and password protect electronic and digital security planning information. Create hard copies in case of a power outage. Retain copies of these plans in a redundant location.
3.3.03	Follow requirements pertaining to the proper handling of Sensitive Security Information (SSI) materials (reference 49 CFR Parts 15 and 1520), such as security plans and risk assessments.
3.3.04	Duplicate all critical documents (e.g., deeds, leases, contacts, local agreements, as-built drawings, manuals, customer records, and personnel records). Duplicates should be stored in a secure off-site location(s).
3.3.05	Shred sensitive documents when no longer needed.
3.3.06	Establish, implement, and maintain security plans to protect computer and information systems, including hardware and software, used to manage the property. Plans include: retaining a riser management company to manage, handle and/or schedule access to the telephone closet; written procedures exist restricting access to the main telephone closet; written procedures exist for the management of floor located telephone closets.
3.3.07	A policy requires computers, portable equipment, and networks to be protected with a unique user identification and system password.
3.3.08	The property has a current listing of all its controlled systems that have an IP address within the building. The property's staff (or through a service agreement with a qualified firm) performs and applies updates to the software programs for each service with an IP address. This includes systems in the management office (i.e. office computers) the building management systems (i.e. BMS/BAS) and the electronic security systems. An outside firm is on retainer to periodically, at least semi-annually, test and confirm that all systems are up to date.
3.3.09	Establish information system security controls (e.g., physical access controls such as locks and guards, intrusion detection sensors and video surveillance) for information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, controlled interface equipment and communications equipment. Segregate telecom equipment in joint use areas to protect against tampering during service calls on other utilities (i.e. cage systems).
3.3.10	Develop a policy for staff regarding business use and the personal use of work computers, including web browsing, e-mail, and social media. Use a tracking program (online or other) to confirm that all onsite staff understand the proper cyber hygiene to be used to operate the property safely.
3.3.11	Immediately cancel (preferably during the exit process) computer and network access for transferred, retired, or terminated employees.
3.3.12	Review electronic information on the building's website periodically to ensure it does not contain any sensitive information (e.g., contact, proprietary, and financial information, technical specification, and chemical and biological storage data). Ensure that the website is protected against unauthorized access or tampering.
3.3.13	Control information on construction activities, including web-cam views. Make construction information available only to authorized personnel.
3.3.14	Save and secure video recordings for forensic purposes per policies set in security plans. Provide video feeds to local law enforcement and other organizations when appropriate.

3.3 Information Security	
3.3.15	Set in place communication security (e.g., encryption, multiple frequencies, countermeasures sweeps) that prevents unauthorized interception of information being transferred. Establish agreement with an outside firm to conduct ongoing monitoring of software systems and generate alerts to the onsite management team. An outside firm is on retainer to periodically, at least semi-annually, test and confirm that all systems are up to date and fit for purpose.
3.3.16	Instruct employees not to discuss sensitive information over unsecure communication channels.

4. Security Systems

4.1 Command Center	
Scope: *Addresses practices that relate to the space in which the site security program is managed.*	
Best Practice: *A designated space on site is used to manage all aspects of the site security program and supports a common operating picture and situational awareness. Alternatives (locations or technologies) are available in case the primary command center is disrupted or incapacitated by an event.*	
Common Security Practices	
4.1.01	The security operations center is staffed by security personnel at all times as determined by the risk assessment. Document this requirement in site security plans.
4.1.02	Designate a workspace in the command center for emergency responders to access emergency plans, building plans, and door control capability.
4.1.03	The security command center has sufficient backup environmental controls (e.g., power, lighting, clean air circulation, etc.)
4.1.04	The command center has access to the facility's public-address system.
4.1.05	The command center can remotely control door locking or unlocking, particularly for stairwells.
4.1.06	Post special alerts (e.g., threat changes, unusual neighborhood activities, terminated employee alerts) in a conspicuous place in the command center.

4.2 Systems

Scope: *Addresses the use of human, animal, and technical systems that assist security personnel to detect, monitor, and control terrorist threats.*

Best Practice: *Electronic, physical, canine, or human systems are implemented to deter and mitigate the threat of an act of terrorism and identify site vulnerabilities*

	Common Security Practices
	Detecting
4.2.01	Install an intrusion detection system around the envelope of the building and on interior areas, where necessary. Use technologies that are based on the facility's risk assessments. Include glass break sensors on windows up to scalable heights, and a roof intrusion detector. Ensure the intrusion detection system is interoperable with the access control system, CCTV cameras, fire safety system, and other relevant security systems etc.
4.2.02	Install automatic sprinkler systems to detect and saturate fire that erupts on site.
4.2.03	Consider using audio analysis to detect suspicious noises (e.g., gunshots and screaming) and to estimate the location of an incident (e.g., shooting, explosion, etc.) through triangulation techniques. Consider the combined use of both video and audio analytics.
4.2.04	Employ canine teams as part of regular or high-visibility patrol teams to detect explosives or other threats.
	Alerting
4.2.05	Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions.
4.2.06	Install an alarm system(s) that can verbally advise building occupants of the appropriate action (e.g., evacuate, shelter-in-place) to take in any event.
4.2.07	Integrate the fire alarm system with other systems (e.g., security, environmental, or building management, etc.) to deliver warnings in tandem or to trigger emergency response during an incident.
4.2.08	Install duress alarms for employees (e.g., call box, intercom, etc.) in locations (e.g., guard stations, interview rooms, manager or supervisor offices, cash and public transaction areas, site-owned vehicles, or other at-risk areas) where people are vulnerable to attack. Employee duress devices should be enabled for immediate response and concealed from the public.
4.2.09	Install duress alarms for the general public (e.g., call box, intercom, etc.) in locations (e.g., parking lots, stairwells, waiting rooms, site-owned vehicles, and other at-risk areas) where people are vulnerable to attack. Public duress devices should be enabled for immediate response and highly visible.
4.2.10	Connect the facility fire alarm system(s) to local emergency services for immediate notification.
4.2.11	The fire command center includes a public-address system.
	Screening, Monitoring, and Surveillance (includes visual inspection of people, assets, and places)
4.2.12	Inspect the person and personal items (e.g., briefcases, backpacks, parcels, luggage, etc.) carried by non-identified people (e.g., visitors, contractors, vendors, etc.) before granting entry into the facility. Use one or a combination of the following inspection techniques: visual and hand searches, metal detectors, x-ray scanners, explosive trace detectors, or canines.
4.2.13	As appropriate, send questionable x-ray images of incoming packages to a remote location where an expert (contractor or vendor) can analyze for detonation material.
4.2.14	Require adequate guard staffing at screening locations to ensure the screening process is performed properly and with an acceptable throughput time. Proper screening may call for one guard to perform only one screening task at a time.

4.2 Systems	
4.2.15	Establish, implement, and maintain procedures for basic screening of vehicles entering parking areas, with a focus on the driver. At a minimum, inspect the trunk, under the hood, and examine the undercarriage of vehicles that enter facility parking areas. Ensure adequate lighting to illuminate the vehicle exterior and undercarriage. Provide CCTV coverage of the screening area.
4.2.16	Spot check vehicles at access points or that are parked for long periods of time in or near the facility.
4.2.17	Move or tow illegally parked vehicles to an appropriate location.
4.2.18	Monitor designated critical areas (e.g., portals, lobbies, the security command center, utility rooms, loading docks, mail room, parking areas, etc.) in accordance with the facility's risk assessments.
4.2.19	Monitor intrusion detection systems (cameras), fire, and other alarms, as well as other building systems from a security command center preferably 24-hours a day or in accordance with the facility's risk assessments.
4.2.20	Use electronic surveillance in locations that provide a view of the building perimeter, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Install cameras at vulnerable access portals. Ensure cameras are interoperable with access control system (i.e., that they respond automatically to interior building alarms and have built-in video motion capability). Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.) and has night vision capability for especially sensitive or critical areas, (e.g., unguarded employee convenience entry doors, rooftops, processing areas, control rooms, communications centers, computer server rooms, shipping areas, mail rooms, fuel or chemical storage tanks, utility access points or service areas, the security operations center, etc.).Interconnect with intrusion, motion, and other detectors (e.g., fire, smoke) as appropriate. Ensure video feeds produce good visual and recording quality. Based on surveillance requirements, assign a sufficient number of security staff to monitor camera feeds. Relieve staff regularly to alleviate fatigue and inattentiveness
4.2.21	Monitor site security employees, facility tenants, contractors, delivery personnel, vendors, etc. for suspicious activities (e.g., irregular work hours, attempting to access restricted areas, carrying unusual packages) or behavior.
4.2.22	Monitor construction work adjacent to the facility (e.g., road construction, utility equipment servicing, etc.) for unusual activities (e.g., placing or planting unusual objects near assets or gathering places).
4.2.23	Monitor elevator areas designed for both employees and visitors.
4.2.24	Conduct nonpredictable but recurring, high-visibility patrols to inspect internal and external areas of the facility (e.g., the site perimeter, including fences and gates, parking lots, equipment, sensitive or critical areas, trash and other containers, etc.). Patrols should question suspicious persons and inspect left-behind packages for explosives and other terrorist weapons as set forth in the facility's security policies and plans.
4.2.25	Use an appropriate number and mix of uniformed and plain clothed security guards to patrol the facility based on the threat level or as determined by risk assessments. For example, increase guard strength during peak hours.
4.2.26	Establish, if applicable, community policing practices with local law enforcement.
4.2.27	Enable, if necessary, remote monitoring of the intrusion detection and alarm systems by authorized authorities.
Access Control - Perimeter	
4.2.28	Protect the facility's perimeter from unauthorized entry as far as practically possible from the building exterior by a physical barrier (i.e., create a buffer zone). Typical perimeter protection barriers include fences, bollards, berms, and concrete walls (Jersey barriers). If necessary, install K12-rated anti-ram bollards around the perimeter of the site or as appropriate.

4.2 Systems	
4.2.29	Bollards should remain in the up position, except for when they are lowered to allow entry of a screened vehicle.
4.2.30	For mechanical locks, use a high-security lock and key system with a minimum of six pins. Ensure that the site's key blank is unique. Consult the risk assessment to determine the appropriate extent of the site's access control system.
4.2.31	Install cameras at critical access portals that trigger an alarm in the command center when a portal is breached.
4.2.32	Instruct security employees not to hold open or block stairways or fire doors during an emergency. Ensure that the fire command center (a.k.a. fire control room, central control station, fire command station, fire control center) includes a public-address system and allows remote locking or unlocking of stairwells.
4.2.33	During an active emergency, security controls that restrict egress through exit doors are automatically deactivated (e.g., activation of a fire alarm, sprinkler system, etc.).
4.2.34	Coordinate access control at the site's perimeter with local law enforcement. Emergency vehicles should have clear access to facility entrances.
Access Control - Personnel	
4.2.35	Change the password for employee keys and PINS periodically.
4.2.36	Display identification badge boards and access documentation at access control points or provide security personnel with sheets and cards showing different identification badges where applicable.
4.2.37	Use security guards (permanent staff or a contract service) to enforce access control. Station access control security guards at main portals and other critical access points in and around the facility.
4.2.38	When security guards are not present, enforce access control at sensitive locations through mechanical or electronic methods.
4.2.39	Incorporate screening equipment and procedures (see, "Screening, Monitoring, and Surveillance" under 4.2 Systems), such as magnetometers (metal detectors), x-ray equipment, etc., at main access portals into the access control system.
4.2.40	The access control system provides an audit trail of ingress into and egress out of the facility and critical areas. Feed real-time audit trail to the facility's command center and main entrance(s) security station to allow for tracking of all site occupants.
4.2.41	Procedures are in place to identify and admit authorized tenants that cannot present facility access identification badges (i.e., for instances where tenants or employees forget to bring identification badges).
4.2.42	Limit tenants' access of facility to public areas and the tenant's own floor(s) through access cards or an appropriate access control method. Ensure that tenants cannot access other tenant space or restricted areas.
4.2.43	Allow tenants to control access to their floor(s) or areas.
4.2.44	The property team has plans in place to gain access to tenant areas for emergency purposes.
Access Control - Vehicles	
4.2.45	Establish, implement, and maintain a system to control access to parking areas commensurate with the facility's risk assessments and security plans.
4.2.46	For unattended or high-volume parking areas, use electronic access control methods to control entry and exit (e.g., automated license plate readers, transponders, biometric readers, electronic card readers, or specially issued stickers or placards).
4.2.47	Install vehicle ingress and egress controls where vehicles and vehicle occupants need to be screened. If necessary, design the vehicular inspection point to include anti-intrusion barriers or vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and to prevent unauthorized exits.

4.2 Systems	
4.2.48	Limit vehicular entry and exits to a minimum number of locations, preferably one.
4.2.49	Remove non-registered or illegally parked vehicles from the premises.
4.2.50	Park or position facility-owned vehicles to block entrances to and exits from the facilities, when appropriate.
4.2.51	Access to the facility is controlled from parking areas inside the facility's envelope.
Utilities and Special Locations	
4.2.52	Control entry to the site during construction so that workers and contractors can only access the parts of the building necessary for construction activities.
4.2.53	Secure all water supplies at all points of entry into the building.
4.2.54	Close and lock secondary or nonprimary entrances during evening or off-peak hours.
4.2.55	Control entry to the site from the loading dock (e.g., use of posted guards, man-trap room, card readers, etc.).
4.2.56	Use an internal messenger or package delivery system to deliver packages to tenants in lieu of external couriers.
4.2.57	Secure all utility tunnels, corridors, manholes, storm water run-off culverts, etc., that could give access to the facility. Lock portals to restricted areas (e.g., utility rooms, hazardous material storage areas, voice and data telecommunication system nodes, etc.) and facility control units (e.g., security system panels, fire command center, elevator panels, fuse boxes, etc.), the roof, and any other critical areas or assets. Consider implementing intrusion detection alarms, balanced magnetic contact switches, timed closure devices, etc., to secure access to critical areas and control units. Ensure that on-site or adjacent auxiliary facilities and services (e.g., utility rooms, maintenance closets, etc.) are secure in accordance with site-specific risk and legal regulations.

4.3 Redundancy and Diversity

Scope: *Addresses the use of human and technical systems to ensure the continued accessibility and operation of critical functions before, during, and after an act of terrorism.*

Best Practice: *Where practical, backups or alternatives for critical utilities and security systems are in place to ensure security program functionality during disruptive conditions. Appropriate technologies are employed to facilitate remote or mobile operations of the security program.*

Common Security Practices	
4.3.01	The facility has adequate utility service capacity to meet normal and emergency needs.
4.3.02	Locate redundant and backup equipment in a different part of the building, where possible, then where the primary supply equipment is located. Replicate command center functions at an alternative site in the building and, if possible, establish an off-site backup that can assume control from the primary security operations center if needed.
4.3.03	Engineer the HVAC system such that independent units are capable of functioning if damage occurs to limited areas of the building.
4.3.04	Set in place, where practical, redundancy and emergency backup capabilities for critical utility services (e.g., backup electric power generators and multiple utility feeder lines).
4.3.05	Set in place an uninterruptible power supply source, battery, or building emergency power for all security systems (access control) and supporting systems (telephone, Internet, etc.).
4.3.06	Provide and document redundancy (multiple supply sources, generators, circuits) in the electrical system for providing continuity of operations such that if a node is disrupted, it would not eliminate both normal electrical service and emergency backup power.
4.3.07	Take actions, to the extent possible, to have the site capable of operating using alternative (nonprimary) fuel supplies.
4.3.08	Establish an alternative (secondary) water supply for fire suppression system and for drinking.
4.3.09	Install redundant fire water pumps (e.g., one electric and one diesel) for the water supply for the fire suppression system.
4.3.10	Alternate sources are available to replenish the drinking water supply.
4.3.11	Create redundancies in the communications system to prevent single points of failure (e.g., have emergency communication equipment like cell phones or emergency radios available for use in the event that all primary channels are unavailable).
4.3.12	Regularly maintain, test and inspect redundant and backup equipment.

4.4 Maintenance

Scope: *Addresses policies and procedures used to ensure the continued accessibility and operation of site functions, especially critical functions, before, during, and after an act of terrorism.*

Best Practice: *Security systems and equipment are installed to function properly. They are kept in good working order and they are regularly inspected, calibrated, and otherwise maintained to applicable standards or regulations (national, state, or local). These activities are documented.*

Common Security Practices	
4.4.01	Set in place a service plan, including preventive maintenance schedules, for all facility security and utility systems.
4.4.02	Prioritize maintenance and repair that could affect the security of facilities such as perimeter fencing, lighting, facility locks, and access points.
4.4.03	Document regular inspections on all life safety systems, including the fire command center, fire extinguishers, smoke and fire control door systems, automatic sprinkler systems, hose cabinets, stairwell exhaust fans, alarms, elevators and escalators, and emergency exits that demonstrate they are functional. Document progress on addressing any open violations until resolved.
4.4.04	Perform regular inspection on any chemical, biological, radiation, and nuclear detection or remediation equipment, particularly in the HVAC system, to ensure it is functional.
4.4.05	Periodically perform maintenance on respiratory protection equipment.
4.4.06	Have all critical security and utility systems inspected or recommissioned according to industry standards or guidance by qualified personnel following a disruptive incident.
4.4.07	Calibrate screening equipment according to the manufacturer's specifications on a regular basis (preferably daily).
4.4.08	Regularly subject major mechanical, electrical, and plumbing systems to a formal recommissioning process, in accordance with industry standards and guidance.
4.4.09	Document the location and capacity of major facility systems (e.g., electrical, mechanical, and fire protection, etc.), such as composite drawings, blue prints, etc.
4.4.10	Maintain, if practicable, in-house staff members to service technological equipment.

5. Communication and Notification

5.1 Policies and Procedures

Scope: *Addresses policies and procedures used to facilitate the site security team's communication with internal and external stakeholders.*

Best Practice: *Policies and procedures ensure that security information is rapidly and efficiently communicated to and from internal and external stakeholders, including sharing of threats and exchange of information with local, regional, and national sites, organizations, first responders, media, government agencies, and others as necessary. The policies and procedures should be based on the site's risk assessment and the risk management process.*

Common Security Practices	
Internal and Site Operations	
5.1.01	Distribute security and emergency response plans to appropriate personnel
5.1.02	Establish security committees for building management to share security information and engage in regular, structured communication with security staff, tenants, and long-term occupants. Invite, when appropriate, personnel from other properties.
5.1.03	Set in place a capability for security personnel (guards) to immediately communicate with one another through communication devices (e.g., portable radio, pager, cell phone, personal data assistants [PDAs]).
5.1.04	Consider adding communication security (e.g., encryption, multiple frequencies) that prevents unauthorized interception of information being transferred.
5.1.05	Identify the frequencies and channels used by local and state police forces for communications. Coordinate use of appropriate frequencies to ensure communication and deter interference.
5.1.06	There are redundancies in the communications system that prevent single points of failure (e.g., have backup emergency communication equipment like cell phones or emergency radios available for use in the event that all primary channels are unavailable).
5.1.07	Alert site occupants immediately to changes in threat level and related changes to security and safety measures. Inform all personnel regularly on the general security situation.
5.1.08	Issue heightened security awareness alerts, including heightened control measures to vendors and contractors.
5.1.09	Use more than one medium (e.g., text message, e-mail, phone, etc.) to disseminate general security information to tenants.
5.1.10	Implement occupant and employee awareness campaigns, such as DHS's "If You See Something, Say Something." campaign, for reporting suspicious behavior and activities.
5.1.11	Establish, implement, and maintain simple, straightforward, and readily available means for personnel to communicate the presence of a threat or an emergency (e.g., panic buttons, hotline number, internal 9-1-1 capability).
5.1.12	Implement a "dispatcher" system in larger facilities for the security guard communications (radio) network. Design the network to ensure adequate coverage throughout the facility and enable users to contact a security operations center regarding tasks, reporting incidents, and requesting assistance.
5.1.13	Establish controls to restrict the release of information that might compromise the security posture of the building.
5.1.14	Instruct employees not to discuss sensitive information over unsecure communication channels.
5.1.15	In the Security Operations Center, on the designated emergency telephone line, record incoming communications (e.g., 9-1-1 telephone calls) to assist response to requests for assistance or to identify potential threats (e.g. bomb threats).

5.1 Policies and Procedures	
5.1.16	Develop a notification protocol that outlines who should be contacted in emergencies, including both building management and tenants.
5.1.17	Install a direct dial phone line in the command center to local authorities and first responders, if necessary.
5.1.18	Provide a special alert notification for recently terminated employees that includes a photograph of the individual to all security staff. Place the alert at all visitor check-in desks.
5.1.19	Establish regular communication channels with utility service providers to discuss infrastructure dependencies, and review existing systems, capacity expansion needs, and actions to be taken in response to loss of service from primary supply sources and other emergencies. Such providers include, but are not limited to electric, gas, water and discharge, IT and telecommunications, trash collection, parking and transportation, and damage restoration and debris removal.
5.1.20	The site's notification system is able to receive rapid alerts or messages from community sources or social media. Ensure security personnel monitor community alerts.
5.1.21	Provide a simple and straightforward means to communicate to site occupants regarding imminent threats or emergency situations.
Community Partners	
5.1.22	Develop rapport and regularly communicate with appropriate local, state, and federal authorities, public health organizations, industry organizations, and other organizations to enhance information exchange, track threat conditions, report suspicious activity, and support investigations.
5.1.23	Share and receive security information (e.g., threat advisories and best practices) through local and regional public and private forums. Premise security forums are often hosted by local police and fire departments, industry groups (e.g., the Building Owners and Managers Association [BOMA] International), area security committees, and state and federal agencies.
5.1.24	Share maps, blueprints, or similar imagery of the physical layout of the facility with appropriate response agencies. Ensure that these maps detail the location of critical assets and relevant site points-of-interest (e.g., water frontage areas, rail lines, emergency access routes, first aid stations, fire hydrants, storage of hazardous material, emergency and utility systems, etc.).
5.1.25	Institute an "open door" policy for area security staff, authorities, first responders, etc., to visit the site and build rapport with the site's security staff.
5.1.26	Invite emergency response services to train and run exercises in the facility during off-hours or weekends.
5.1.27	Use, when practicable and beneficial, the same administrative and training assets (e.g., joint training, joint grant writing, etc.) with appropriate organizations.
5.1.28	Share external camera feeds with local authorities where available or permissible.
Media	
5.1.29	Assign specific employees to interact with the media and to deal with the public in the event of an incident. Ensure that these employees are well versed with site security plans and protocols, participate in all training exercises, and are aware of legal reporting requirements during incidents.
5.1.30	Establish and use templates for press releases and written communication to the public. Ensure that all templates are pre-approved by site legal counsel.

5.2 Signage and Announcements

Scope: *Addresses policies and procedures related to the use of communication aids by the site security team before, during, and after an act of terrorism.*

Best Practice: *Clear, simple communication (e.g., physical signs, public address announcements, and other notification techniques) is made to internal or external stakeholders on site security information, policies, and procedures in accordance with applicable regulations, codes, and the site security program.*

Common Security Practices	
5.2.01	Display prominently security awareness and emergency preparedness information materials throughout the facility using appropriate signs, channel cards, posters, fliers, etc. Post security awareness and emergency preparedness information as appropriate on the building's website.
5.2.02	Design text and finishes on signs for clarity and ease of reading.
5.2.03	Display identification badge and access information at access control points and provide personnel with sheets and cards with identification badge and access information.
5.2.04	Ensure all site signage is durable against human tampering and natural weather events.
5.2.05	Provide a simple and straightforward means to communicate to site occupants regarding imminent threats or emergency situations.
5.2.06	Post signage that informs site occupants that personal items, including packages, briefcases, purses, backpacks, parcels, luggage, etc., may be subject to inspection.
5.2.07	Post signage on the perimeter of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.).
5.2.08	The identification and location of critical assets in the facility should not be obvious to the general public.

6. Defensible Space Design

6.1 Physical Structure

Scope: *Addresses policies and procedures related to the design, construction, operation, and retrofitting of all structures and related exterior infrastructure, as well as interior technical systems, covered by the site security program.*

Best Practice: *The physical structure of the site and security systems are designed and hardened to meet or exceed the risks identified for the facility and the requirements (state and local codes and regulations) in place at the time of original construction. New facilities, new additions, and areas undergoing major renovations meet or exceed the risks identified at the time of new construction and comply with current codes and regulations. A CPTED approach is used for space design. Physical protections add structural resilience and secure and enhance security systems on an ad hoc basis, as the need arises.*

	Common Security Practices
6.1.01	Design the building to promote a sense of implemented security measures, the presence of security staff, reduced areas of concealment, continuous monitoring, controlled access and appropriate responsive measures. Example proofs of intent include plans, elevations and photographs showing clear lines of sight for security stations, eliminated blind corners, appropriate illumination, maximized security visibility, natural barriers, separation of protected spaces, etc.
6.1.02	Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.
6.1.03	Glass in high-risk areas is designed in accordance with relevant standards and to meet the security requirements of the threat(s), threat locations and vulnerabilities of the risk assessment. Reference: American Society for Testing and Materials (ASTM) F 1642-12 (current version) "Standard Test Method for Glazing and Glazing Systems Subject to Air Blast Loadings."
6.1.04	Refuge or shelter in place areas should be designed in the facility. These areas should be well protected through use of location, appropriate enclosure and security systems.
6.1.05	Minimize egress between residential areas and nonresidential areas if the site is mixed-use. Seal off all residential areas from all restricted areas without compromising the facility's fire life safety practices.
6.1.06	For high ceiling heights (over 16 feet), discontinuous columns, long spans and other potential structural deficiencies conduct and document a thorough structural review.
6.1.07	Areas containing critical assets should be protected through effective location, and appropriate enclosure and security systems.
	Reinforcement/Protection
6.1.08	Design the building enclosure and structure to withstand blast loads and progressive collapse related to identified threats from the site risk assessment. Current building code natural hazards loadings should be documented, and additional blast loads calculated and designed into the building. Example proofs of level of protection provided that should be available for inspection include structural calculations and analysis of blast loading for the enclosure and structural systems, and progressive collapse evaluation for the building structural system.
6.1.09	Mark front and rear facility doors with the facility's address, on or above the doors. Peepholes should be designed into exterior doors to enhance surveillance of the facility's exterior.
6.1.10	Securely anchor exterior doors to a structure using a metal frame that is grouted with cement.
6.1.11	Mount exterior doors to ensure that they open outward-that is, away from an interior space.
6.1.12	Install hinges on the door interior to prevent removal of exterior doors from the hinge side, provide concealed hinges, and use heavy-duty grade with nonremovable pins. If removable pins are installed, weld them in place to prevent their removal and reduce their vulnerability to tampering.

6.1 Physical Structure	
6.1.13	Use industry standard ballistic level protection rating to specify unglazed exterior doors that require ballistic-level protection.
6.1.14	Ensure high-risk-area doors use ballistic protections against adversary actions to penetrate the opening.
6.1.15	Install interior glass that is shatter-resistant (e.g., the glass is glazed or is fully tempered safety glass that can withstand a pressure of 16,000 psi).
6.1.16	Secure nonwindow openings greater than 96 square inches in perimeter walls with grilles, bars, or alarms.
6.1.17	Mount overhead objects (light fixtures, etc.) weighing 31 pounds (14 kilograms) or more using either a rigid or flexible system to minimize likelihood of falling. Suggested mounting systems will resist a downward force of 1.5 times the weight of the object and 0.5 the object's weight in a horizontal direction.
6.1.18	Secure ladders, awnings, and parapets that give access to building roofs, HVAC systems, and other critical equipment. Limit and trim nearby foliage (e.g., trees, shrubs) so it cannot be used to gain access to the roof.
6.1.19	Doors and walls along the line of security screening meet requirements of UL 752 "Standard for Safety: Bullet-Resisting Equipment."
6.1.20	Secure incoming communication equipment (telephone, Internet, etc.) from external tampering by placing transformers or switchgears where they are not accessible from outside the building.
6.1.21	Harden enclosures and pathways for emergency egress to limit the extent of debris that might impede safe passage and reduce the flow of evacuees.
6.1.22	Fenestration glass, particularly to scalable heights, should be suitably protected (e.g., by glazing) against impact and shattering into shards, per the facility's risk assessment.
6.1.23	Cameras have housings designed to protect them against exposure or tampering.

6.2 Protected Areas

Scope: *Addresses policies and procedures related to the design, construction, operation, and retrofitting of all public spaces, including interior spaces, covered by the site security program.*

Best Practice: *Based on the identified risk, areas open to the public where access is monitored, limited, or controlled are designed and located to enhance detection and apprehension of illicit activity as well as to mitigate consequences from an act of terrorism.*

Common Security Practices	
Portals (entry and exit)	
6.2.01	Locate, if site allows, pedestrian access control and inspection points at the perimeter of the site, as far from the facility as possible.
6.2.02	Locate vehicle access control and inspection points at the perimeter of the site, as far from the facility as possible.
6.2.03	Locate guard stations and kiosks so that site staff and security officers have optimum sight lines into and out of portal areas.
6.2.04	Use single- or double-leaf configurations and commercial security hollow metal exterior doors (exterior doors) as the facility's general public entrance and exit doors or as service entrances for facility operations personnel.
6.2.05	Limit the number of exterior doors to reduce the number of vulnerabilities to the facility's envelope.
6.2.06	Install automatic door closers and locks on the outside of exterior doors other than the main lobby entrance. Automatic locks must not restrict evacuation during emergency conditions.
Lobby, Concourse, and Waiting Areas	
6.2.07	Conduct visitor screening where site configuration allows in an area outside the main building footprint to prevent incidents in the lobby from impacting the rest of the facility.
6.2.08	If possible, design the lobby or waiting areas to increase throughput (reduce queuing) while maintaining the effectiveness of the security measures. Reduce queuing time in these areas by maximizing the number of visitor receptionists, screening lanes, and the processing speed of access control systems.
6.2.09	Minimize public restrooms in nonsecure areas. Locate public restrooms away from the main facility entries and exits.
Stairwells	
6.2.10	Locate stairways for emergency egress as remote as possible from high-risk areas, and design them to discharge into areas other than lobbies, parking zones, or loading docks.
6.2.11	Use different stairwells for evacuation and for "attack" by first responders, install fire hose connectivity in "attack" stairwell(s), and use double-wide stairwells for "evacuation" stairwell(s).
6.2.12	Eliminate potential hiding places (nooks and crannies) below stairways.
Elevators	
6.2.13	Install CCTV in all freight elevators. If necessary, install cameras in public elevators.
6.2.14	Install an emergency message capability on elevators.
Parking	
6.2.15	Design, as site configuration allows, parking areas adjacent to or as far from the facility and critical assets as practicable. Limit parking areas inside the facility's envelope.
6.2.16	Locate vehicle access control and inspection points at the perimeter of the site as far from the facilities as possible.
6.2.17	Establish and enforce a minimum setback and standoff distance between the facility envelope and parked vehicles. (For guidance, consult the DHS Science and Technology's Building and Infrastructure Protection Series [BIPS] publication BIPS-06 "Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.")

6.2 Protected Areas	
6.2.18	Parking garages and parking lots should be located and designed to present the lowest number of vulnerabilities to the building and occupants.
6.2.19	There is adequate visibility (line-of-sight or cameras) across, into, and out of parking lots and garages.
6.2.20	Separate visitor parking from occupant parking.
6.2.21	Establish controls so that vehicles are not left unattended in driving lanes that are closer to the buildings than the required standoff distance set for the facility.
6.2.22	Design stair and elevator waiting areas of parking structures such that they are visible to the exterior and keep parking areas well lit.
6.2.23	Control curb-lane parking such that unauthorized vehicles are not allowed to park close to a building.
6.2.24	Allow no dead-end parking areas in parking lots that are within the standoff distances set for the facility.
Vehicle/Pedestrian Channels	
6.2.25	Design traffic patterns to ensure circulation that prevents high-speed approaches by visitors; barriers, planters, and landscaping may be useful.
6.2.26	Provide an interior perimeter road for patrols where the perimeter barrier (e.g., fencing) encloses an area generally greater than 1 square mile (2.6 km2). Drainage culverts passing under the road in clear zones must be secured at all openings for drainage and culverts under fences.
6.2.27	Perform periodic maintenance of the perimeter roadway to prevent or remove overgrown vegetation, trees, or shrubs, ensure snow or other debris removal, maintain an unobstructed line of sight along the property boundary, and prevent damage to vehicles using the road.
Lawns and Grounds	
6.2.28	Install landscaping to be a physical barrier for the building and obstruct view angles (take care not to create hiding places), but not to obstruct the lines of sight to see pedestrians or vehicles approaching the building.
6.2.29	Utilize landscaping and other site features to provide for effective surveillance and reduce opportunities for concealment or entry into the facility.
Restrooms	
6.2.30	Publicly accessible restrooms are key locked and use a key control system. If there is a combination lock, only authorized personnel should open the lock for visitors.
Miscellaneous Areas	
6.2.31	Protect and secure onsite or adjacent auxiliary facilities and services (e.g., day care center) consistent with the security plan.

6.3 Controlled and Restricted Areas

Scope: *Addresses policies and procedures related to the design, construction, operation, and retrofitting of all nonpublic spaces covered by the site security program.*

Best Practice: *Based on the identified risk, areas on the premises where access is strictly or tightly controlled are designed and located to enhance detection and apprehension of illicit activity as well as to mitigate consequences from an act of terrorism.*

Common Security Practices	
Roof	
6.3.01	Lock and secure all portals that allow access to the roof. Limit roof access to authorized personnel only.
6.3.02	Install an intrusion detection system on the roof.
6.3.03	Secure ladders, awnings, and parapets that give access to building roofs, HVAC systems, and other critical equipment.
Storage	
6.3.04	Secure onsite or adjacent auxiliary facilities and services (e.g., utility rooms, maintenance closets, etc.) according to site-specific risk and legal regulations.
6.3.05	Store all hazardous chemicals, flammable or toxic materials, and fuel supplies that must be kept on-site in secured and monitored areas. Handle in compliance with state and local regulations.
6.3.06	Store all hazardous chemicals, flammable or toxic materials, and fuel supplies that must be kept onsite away from loading docks, portals, and parking areas. Handle in compliance with state and local regulations.
Mail Room	
6.3.07	Locate the mail room away from main entrances and areas containing critical infrastructure, utilities, distribution systems, and other important assets.
6.3.08	Locate the mail room at the perimeter of the building with an outside wall or window designed for pressure relief.
6.3.09	Limit delivery times during peak business hours. Schedule as many deliveries as possible for times when the building is not open to the public, such as the early morning or weekends.
6.3.10	Require mail room screening of all packages delivered to the transit hub. Packages include, but are not limited to, U.S. mail, commercial package delivery services, and delivery of office supplies.
6.3.11	Separate mail room ventilation from the site's central ventilation system.
6.3.12	Equip mail rooms with detection equipment and isolation equipment capable of screening and identifying CBRN materials.
6.3.13	Train receiving personnel (and staff of mail rooms and mail boxes) to recognize suspicious mail, packages, shipments, or deliveries, including instruction on the following notification procedures: Inspect all packages and mail for unusual signs such as leaking powders, strange odors, no return address. Direct suspicious packages and mail to a controlled area for handling. Provide personal protective equipment for those handling suspicious packages and mail.
Loading Dock	
6.3.14	Post a security officer at the loading dock at all times. At the very least, post a security officer during normal facility hours and during any after-hours dock activity.
6.3.15	Design and locate loading dock areas to keep unauthorized vehicles from driving or parking in or under the building.
6.3.16	If the loading dock is shared with adjacent facilities, ensure that one site's security staff controls security operations.
6.3.17	Control entry to the site from the loading dock through the use of "man-trap" doors.

6.4 Accessories

Scope: *Addresses policies and procedures related to the design, construction, operation, and retrofitting of all interior fixtures and other accessories (excluding security systems) covered by the site security program.*

Best Practice: *Based on the identified risk, site accessories (e.g., trash cans, vending machines, water fountains, mailboxes, aesthetics, newspaper stands, bike racks, etc.) are designed and located to reduce the risk of the object being used as a terrorist tool as well as to mitigate consequences from an act of terrorism.*

Common Security Practices	
6.4.01	Aesthetic displays (e.g., posters, advertisements, etc.) do not obstruct visibility into or out of critical areas.
6.4.02	Eliminate the use of containers in which left-behind packages or other items may be hidden.
6.4.03	Inspect and closely monitor site decorations (e.g., Christmas displays, etc.) and charitable collection boxes that can be used to conceal weapons and explosives, particularly during holiday seasons.
6.4.04	Use bomb-resistant receptacles or clear plastic containers to hold trash or disposables. Openings should allow only the insertion of items smaller than six inches (150 mm) in height or width.
6.4.05	Receptacles are frequently emptied.
6.4.06	Enclose and secure dumpsters or other large containers used for site operations.
6.4.07	Keep all exterior site accessories at least 33 feet (10 meters) away from the facility envelope.
6.4.08	Emergency vehicles should have clear access to all fire hydrants, standpipes and facility entrances.
6.4.09	Allow only vending machines with no holes and that have sloped tops to reduce the likelihood that a bomb can be hidden in or placed on top of the machine.

6.5 Utility Systems and Equipment

Scope: *Addresses policies and procedures related to the design, construction, operation, and retrofitting of all exterior and interior utility systems covered by the site security program.*

Best Practice: *Based on the identified risk and assessment of the cost-benefit, utility systems (HVAC, electrical, etc.) are designed and located to reduce the risk of their use as a terrorist tool as well as to mitigate consequences from an act of terrorism.*

Common Security Practices	
General	
6.5.01	Consider the security of the physical location of critical assets when planning and performing new construction or major renovations.
6.5.02	Place critical assets (safes, fuel supplies, computer servers, HVAC system, fire life safety control system, command center, etc.) in secure areas away from vulnerable areas, such as portals, vehicle circulation areas, areas of congestion, parking, maintenance areas, loading docks, or utility systems.
6.5.03	Locate redundant and backup equipment in a different part of the building than primary equipment.
6.5.04	Locate utility supply facilities and equipment that are potentially hazardous (e.g., liquid fuel tanks, high-voltage power lines) at a safe distance from the building or in areas where large numbers of people congregate. Locate these supplies off-site, if possible.
6.5.05	Protect nonwindow openings, such as mechanical vents and exposed plenums so that they provide the same level of protection required for the exterior wall. Install lighting around the facility's perimeter.
Air Supply	
6.5.6	Locate fresh air intakes on the fourth floor or as high as practical (fifty feet above ground is recommended). Location on a wall is preferred over a roof.
6.5.7	Design fresh air intakes so that debris rolls off (e.g., cover openings with screens or slope them downward).
6.5.8	The HVAC system can sustain other systems (e.g., servers, fire command center, etc.) that require temperature and humidity control.
6.5.9	HVAC and the exhaust system are designed for rapid shutdown.
6.5.10	Establish HVAC zones for lobbies, mail rooms, loading docks, and other entry and storage areas that can maintain negative pressure to contain releases of CBRN materials.
6.5.11	Air intakes and exhausts are closed when not operational.
6.5.12	Install air monitors or sensors for CBRN agents in the air handling system.
6.5.13	Filter HVAC exhaust using, for example, high efficiency particulate arrester (HEPA) filters.
6.5.14	Install, to the extent possible, multiple air intake locations.
Electrical Supply and Telecommunications	
6.5.15	Install more than one entry point for electrical service to the facility.
6.5.16	Use ducts and other conduits to run utility service through the facility.
6.5.17	Install redundant nodes in the electrical system such that if a node is disrupted, it would not eliminate both normal electrical service and emergency backup power.
6.5.18	Have electrical service provided from at least two different sources (i.e., substations) where possible.
6.5.19	Have in place two minimum-points-of-presences (MPOPs) for communication equipment.

7. Performance Evaluation

7.1 Exercising and Testing

Scope: *Addresses policies and procedures related to the exercise of all functions under the site security program, as well as the testing of related equipment and systems to ensure proper functionality.*

Best Practice: *Security plans and procedures are regularly practiced or exercised to ensure that they function in accordance with security program objectives and the Homeland Security Exercises and Evaluation Program (HSEEP). When possible, exercises incorporate all tenants and responding agencies, and address issues of unified command and control. Security systems and equipment are regularly tested to assure they function as intended. Exercise and testing activities are documented.*

Common Security Practices	
General	
7.1.01	Instill a security culture of periodically exercising all security related plans, procedures, and products.
7.1.02	Document the dates and outcomes of all exercises or tests of security plans, procedures, and products.
Exercising	
7.1.03	Regularly exercise property team and security staff on aspects of site security plans.
7.1.04	Exercise the communication and notification plan. Ensure a simple and straightforward means for people to send and receive information regarding a potential threat or an emergency.
7.1.05	Exercise facility emergency procedures periodically with building occupants. Vary exercises to test all types of foreseeable incidents. Evaluate all exercises and immediately inform appropriate personnel and all site occupants of any changes.
7.1.06	Invite neighboring buildings to participate in emergency drills and training exercises to extend knowledge and outreach should emergencies occur.
7.1.07	Invite local law enforcement and emergency responders to participate in emergency drills and training exercises to familiarize them with the building and its security and emergency procedures.
Testing	
7.1.08	Test periodically all access control devices (e.g., electronic readers) to be sure they are providing timely and accurate (proper identity verification) access.
7.1.09	Test periodically all video equipment to ensure clear lines-of-sight and to ensure they otherwise proper functionality, including the ability to record and time and date stamps.
7.1.10	Test periodically all emergency response equipment according to manufacturer instructions.
7.1.11	Test periodically all life safety systems, including fire extinguishers, alarms, elevators and escalators, and emergency exits to ensure functionality. Ensure that lighting along evacuation paths is functional when normal power is interrupted.
7.1.12	Test periodically all contact databases, calling trees, notification and recall lists, and other communications lists.

7.2 Evaluation

Scope: *Addresses policies and procedures related to the formal and informal assessment and improvement of all exercises, tests, and incidents related to the site security program.*

Best Practice: *Security program procedures and capabilities are evaluated for suitability, adequacy, and effectiveness through periodic reviews, post-incident reporting, and performance evaluations, applying metrics where relevant. The method of evaluation is in accordance with the Homeland Security Exercises and Evaluation Program (HSEEP). This responsibility is assigned by top management to an individual and conducted without influence of top management. Evaluations are used to inform and make recommendations to top management regarding the status of the security program, appropriate corrective actions, and opportunities for continuous improvements. An internal audit of the security program is conducted by a qualified individual periodically, typically annually. This audit is conducted free of top management influence and is independent of other evaluation activities.*

Common Security Practices	
7.2.01	Conduct security program audits at least annually. Ensure a security review committee (or other designated group) addresses the findings and recommendations from audits, and updates plans, protocols, and processes as necessary.
7.2.02	Have local law enforcement or a qualified third- party vendor perform a security audit of the building.
7.2.03	Develop site-specific performance measures that measure the effectiveness of the security program. Compare current performance to past performance. Examples include: degree of a security activity's implementation; the number of risk assessments completed during a calendar year; determining the security program's effect on risk over time; documenting and analyzing the frequency and impact of security-related incidents over time; and the number of access control failures.
7.2.04	Where possible, conduct comparisons of performance measures with external properties.
7.2.05	Establish a self-assessment competency to provide internal audits of program implementation and outcomes.
7.2.06	Document all incidents that occur at the site or are relevant to the site's security environment.
7.2.07	Evaluate periodically incident reports to determine if changes in site security policy, procedure, or practice are needed.
7.2.08	Prepare after action reports on emergency drills and exercises. Use these reports to inform improvements to the security system and as documentation that the exercise was conducted.
7.2.09	Prepare an after-action report for incidents that breech security. Determine circumstances that led to successful attack. Evaluate response performance. Identify and implement corrective measures. Document actions and lessons learned.
7.2.10	Review and evaluate the recovery plan periodically (e.g., through table-top exercises, etc.). Invite appropriate external stakeholders to participate.