

Security Guidance for Commercial Buildings

District of Columbia Homeland Security and Emergency Management Agency

2720 Martin Luther King, Jr. Avenue, SE

Washington, DC 20032

202-727-6161

April 2012

GOVERNMENT OF THE DISTRICT OF COLUMBIA



Dear District Homeland Security Partner,

The Homeland Security and Emergency Management Agency (HSEMA) is dedicated to sharing information to facilitate prevention, protection, response to, and recovery from all-hazards that might impact the District. As an owner or operator of a commercial facility in the District, you are a critical partner in ensuring a safe and secure District of Columbia.

The information included in this document identifies potential indicators of terrorist activity, common vulnerabilities of commercial facilities, potential protective measures, and useful references. We encourage you to use the informational guidelines in this document to consider new and improved ways to enhance the security of your building.

Thank you for working to help us realize a safe and secure District of Columbia.

For more information, please contact:

DC Homeland Security and Emergency Management Agency

2720 Martin Luther King Jr. Avenue, SE

Washington, D.C. 20032

202-727-6161

www.hsema.dc.gov

Table of Contents

Introduction.....	1
Real Estate - Office Buildings, Condominiums, Self-Storage Facilities.....	3
Public Assembly	5
Convention Centers.....	5
Museums, Zoos, Libraries.....	7
Parades, Festivals, Rallies	9
Stadiums and Arenas.....	12
Lodging - Hotels, Motels, Conference Centers.....	14
Performance Venues – Theaters, Concert Halls, etc.....	16
Retail - Shopping Malls, Retail Centers.....	18
Mail and Package Handling Facilities.....	20
Child Care Centers.....	22
Nursing Homes	24
Residential Buildings.....	26
Active Shooter - How to Respond	28
Profile of an Active Shooter.....	28
When an Active Shooter Is In Your Area	29
When Law Enforcement Arrives	30
Training Your Staff.....	31
Preparing For and Managing the Situation	32
Recognizing Potential Workplace Violence	33
Managing the Consequences.....	33
Suspicious Packages and Mail	35
Bomb Threat: Stand-Off Chart	36
Shelter-in-Place.....	38
At Home.....	38
At Work	38
At School	39
In Your Vehicle	40
Shelter-in-Place: Business	40
Alert DC System.....	53
Emergency Go-Kit Information	54

DISCLAIMER

The enclosed suggestions should not replace the advice of trained medical staff and police officials. All data compiled here is for informational purposes only and HSEMA, its employees, and affiliates do not accept responsibility for any injury, loss or damage arising from the use of this information. During a time of crisis, citizens should heed the advice of local officials over the data contained in this reference material.

Real Estate – Office Buildings, Condominiums, Self-Storage Facilities



Commercial office buildings range in size from less than 1,000 to more than 1 million square feet. About 2,000 buildings in the United States (less than 1% of the total number) have more than 500,000 square feet of floor space, and about 7,000 (nearly 1%) have more than 200,000 square feet. The amount of space in these larger buildings is significant: nearly 30% of all commercial office floor space is in buildings with more than 200,000 square feet.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to commercial office buildings include:

- Improvised explosive devices
- Arson
- Small arms attack
- Assassination/kidnapping
- Chemical/biological/radiological agent attack
- Aircraft attack
- Cyber attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas wearing unusually bulky clothing that might conceal suicide explosives
- Vehicles illegally parked near facility buildings or near places where large numbers of people gather
- Unattended packages (e.g., backpack, briefcase, box) that might contain explosives
- Suspicious packages and/or letters received by mail that might contain explosives or chemical/biological/radiological agents

- Evidence of unauthorized access to HVAC areas of a building

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment in or near the facility over an extended period
- Persons discovered with facility maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- Persons questioning facility employees off-site about practices pertaining to the facility and its operations, or an increase in personal e-mail, telephone, faxes, or postal mail requesting information about the facility or one of its key assets
- Facility employees inquiring about facility operations, equipment, assets, or security measures about which they should have no job-related interest
- An increase in buildings left unsecured or doors left unlocked, when normally secured and locked at all times

Common Vulnerabilities

The following are key common vulnerabilities of commercial office buildings:

- Lack of adequate perimeter and site security measures (e.g., fences, bollards, security cameras)
- Building designs that lack security considerations (e.g., blast-resistant glass)
- Lack of adequate vehicular control (e.g., traffic control, parking area controls)
- Lack of security in loading docks, shipping and receiving areas, mailrooms
- Open access to buildings by tenant employees, visitors
- Lack of security at HVAC systems
- Lack of security at building utility supply points
- Limited emergency response and security forces
- Lack of security regarding food suppliers

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for commercial office buildings include:

• Planning and Preparedness

- Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits. Develop a comprehensive security plan and emergency response plan for the facility.
- Conduct regular exercises with facility employees, including building management and tenants.
- Establish procedures for building evacuation and for shelter-in-place situations.

• Personnel

- Conduct background checks on all employees.
- Incorporate security into employee training programs conducted for building management and tenants.
- Maintain an adequately sized, equipped, and trained security force. Conduct regular drills.

• Access Control

- Issue photo identification badges to all employees. Require that badge be displayed.
- Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees.
- Require sign-in/sign-out for visitors. Issue special identification badges to visitors.
- Review vehicle traffic patterns inside the building parking areas. Keep vehicles distant from sensitive or critical areas.
- Approach all illegally parked vehicles. Require that they be moved or have them towed.
- Provide adequate door and window locks and other access controls to areas where access is to be limited. Add intrusion detection systems and alarms.
- Train mail room and receiving personnel to recognize suspicious mail, packages, shipments, or deliveries.

• Barriers

- Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility.
- Install barriers to protect doors and windows from small arms fire and explosive blast effects.
- Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from critical areas.

• Communication and Notification

- Install system(s) that provide communication with all people at the facility, including building management and tenant employees.
- Develop a notification protocol that outlines who should be contacted in emergencies, including both building management and tenants.

- Develop a process for communicating to building management, employees, and tenants the current security situation.

• Monitoring, Surveillance, Inspection

- Install video surveillance equipment (e.g., closed-circuit television [CCTV], lighting).
- Install detector and alarm systems.
- Continuously monitor all people entering and leaving the facility.
- Continuously monitor all vehicles approaching the facility for signs of threatening behavior.

• Infrastructure Interdependencies

- Ensure that the facility has adequate utility service capacity to meet normal and emergency needs. Identify all utility service points that support the facility.
- Establish regular communication channels with utility service providers.

• Cyber Security

- Develop and implement a security plan for computer and information systems. Design and implement a secure computer network architecture.
- Regularly review the facility's Web site to ensure no sensitive information is provided.

• Incident Response

- Ensure that an adequate number of building management emergency response personnel are on duty and/or on call at all times.
- Provide training and equipment to building management emergency response personnel to enable them to deal with terrorist-related incidents.

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Public Assembly – Convention Centers



The United States has more than 600 convention centers and many more hotels that contain conference/convention centers. Facilities included in this number range from large, multi-functional urban structures, to stand-alone exhibition/exposition centers, to buildings at state and local fairgrounds, to sports arenas. Convention centers are located in every region of the United States and in almost all states. The Walter E. Washington Convention Center is considered the third busiest in the nation.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to convention centers include the following:

- Improvised explosive devices
- Arson
- Chemical/biological/radiological agents
- Small arms attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., registration areas, popular exhibition spaces) wearing unusually bulky clothing that might conceal suicide explosives; weapons (e.g., automatic rifle) may also be concealed under their clothing
- Unattended vehicles illegally parked near convention center buildings or places where large numbers of patrons gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to heating, ventilation, and air conditioning (HVAC) areas; indications of unusual substances near air intakes

Indicators of potential surveillance by terrorists include the following:

- Persons using or carrying video/camera/observation equipment over an extended period
- Persons discovered with a suspicious collection of convention center maps, photographs, or diagrams with facilities highlighted
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- Employees being questioned off-site about practices pertaining to the convention center
- Employees changing working behavior or working more irregular hours
- Persons observed or reported to be observing convention center receipts or deliveries
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar cleaning crews or other contract workers
- An increase in buildings left unsecured or doors left unlocked
- An increase in threats from unidentified sources
- Unusual or unannounced maintenance activities in the vicinity of the convention center
- Sudden losses or thefts of guard force equipment

Common Vulnerabilities

The following are key common vulnerabilities of convention centers:

- Unrestricted public access
- Large number of access points
- Unrestricted access to areas adjacent to buildings
- Access by suppliers, vendors, and maintenance workers to nonpublic areas
- Limited employee background checks
- Limited security force
- Lack of exercises for emergency plans

- Unprotected HVAC systems and utility services
- Building designs that are not security oriented
- Multiple locations to place explosives or hazardous agents

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for convention centers include the following:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan based on threat analyses, vulnerability assessments, consequence analyses, and risk assessments
- Conduct regular exercises of the plans
- Establish liaison and regular communication with local law enforcement and emergency responders
- Instruct event organizers on emergency preparedness and response during pre-event phase

• Personnel

- Conduct background checks on convention center employees
- Incorporate security awareness and appropriate response procedures for security situations into employee training programs
- Maintain an adequately sized, equipped, and trained security force

• Access Control

- Provide appropriate signs to restrict access to non-public areas
- Identify and control access by all employees, vendors, delivery personnel, contractors, and patrons
- Install and regularly test electronic access control systems and intrusion detection systems in sensitive areas
- Identify key areas in or adjacent to convention center buildings and control vehicle access/parking there

• Barriers

- Provide adequate locks, gates, doors, and other barriers for designated security areas
- Install and inspect blast-resistant trash containers
- Install barriers at HVAC systems to prevent the introduction of chemical, biological, or radiological agents into the convention center
- Install active vehicle crash barriers at selected areas to protect buildings and populated areas

• Communication and Notification

- Install, maintain, and regularly test the facility security and emergency communications system
- Develop redundancy in the facility security and emergency communications system

- Provide and periodically test redundant communication channels with local law enforcement and emergency responders
- Develop process for communicating with the patrons, public, and media regarding security-related incidents
- Provide simple means for reporting any situation or suspicious activity that might constitute a threat

• Monitoring, Surveillance, Inspection

- Install closed-circuit television (CCTV) and intruder detection systems and lighting to cover key areas
- Train security personnel to watch for suspicious or unattended vehicles on or near facilities; repeated visitors or outsiders who have no apparent business in non-public areas of the convention center; abandoned parcels, suitcases, backpacks, and packages and unusual activities; and utility supplies and routine work activities scheduled on or near assets
- Regularly inspect trash bins, parking lots and garages, and all designated security areas

• Cyber Security

- Develop and implement a security plan for computer-based operational systems
- Regularly test the computer security measures
- Eliminate any information from Web site that might provide security information to adversaries

• Infrastructure Interdependencies

- Provide adequate capacity, redundancy, security, and backup for critical utility services (e.g., electricity, natural gas, water, telecommunications) for normal and emergency needs
- Provide for regular monitoring and inspection of utility services (e.g., security force patrols, CCTV) and testing of backup capability

• Incident Response

- Identify entry and exit points to be used in emergencies and regularly inspect them

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Public Assembly – Museums, Zoos, Libraries



The Smithsonian Institution—the world's largest museum and research complex—includes 19 museums and galleries and the National Zoo. The Smithsonian welcomed more than 28.6 million visitors in 2011. Of those, 6.6 million were to the Museum of Natural History, which houses the Hope Diamond, a security concern unto itself. In addition to the 25 locations for the DC Public Library system, there are numerous university libraries and law libraries throughout the city that receive hundreds of visitors on a daily basis.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to museums, libraries, zoos, planetariums, and aquariums include those that involve:

- Improvised explosive devices
- Arson
- Small arms attack
- Chemical, biological, or radiological agents

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., common areas, food courts) wearing unusually bulky clothing that might conceal suicide explosives or hide weapons (e.g., automatic rifle)
- Unattended vehicles illegally parked near buildings or places where large numbers of patrons gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to heating, ventilation, and air-conditioning (HVAC) areas; indications of unusual substances near air intakes

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment over an extended period
- Persons having maps, photos, or diagrams with facilities highlighted
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation for doing so
- Persons questioning employees off-site about practices pertaining to the facility
- Employees changing working behavior or working more irregular hours
- Persons observed or reported to be observing facility receipts or deliveries
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar cleaning crews or other contract workers
- An increase in the number of incidences when buildings are left unsecured
- An increase in threats from unidentified sources
- Sudden losses or thefts of guard force equipment

Common Vulnerabilities

The following are key common vulnerabilities of museums, libraries, zoos, planetariums, and aquariums:

- Easy accessibility of facilities to large numbers of public patrons
- Accessibility of items having unique value and/or significance
- Presence of dangerous animals in zoos

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for public institutions include:

- **Planning and Preparedness**

- Develop comprehensive security and emergency response plans and conduct regular exercises of the plans.
- Maintain a constant awareness of the current threat condition and available intelligence information.
- Establish liaisons and regular communications with local law enforcement and emergency responders.

- **Personnel**

- Conduct background checks on all employees.
- Incorporate security awareness and appropriate response procedures for addressing security situations into training programs.
- Maintain an adequately sized, equipped, and trained security force.
- Check training rosters to ensure that personnel have received proper training on the Homeland Security Advisory System and specific preplanned measures.

- **Access Control**

- Provide appropriate signs to restrict access to nonpublic areas.
- Identify and control access by all employees, vendors, delivery personnel, and contractors.
- Install electronic access control systems and intrusion detection systems in sensitive areas.
- Identify key areas in or next to buildings and prohibit parking in these areas.
- Issue photo identification badges to all employees and require that badges be displayed at the facility.

- **Barriers**

- Provide adequate locks, gates, doors, and other barriers for designated security areas.
- Inspect barriers routinely for signs of intrusion.
- Install barriers at HVAC systems, hatches, and power substations and routinely patrol these areas.

- **Communication and Notification**

- Install, maintain, and regularly test the facility security and emergency communications system.
- Communicate threat level information to employees.
- Take any threat (phone, fax, e-mail) seriously.
- Encourage employees and the public to report any suspicious activity that might constitute a threat.

- **Monitoring, Surveillance, Inspection**

- Install closed-circuit television (CCTV) systems, intruder alarms, and lighting to cover key areas.

- Train security personnel to watch for repeated visitors or outsiders who have no apparent business in nonpublic areas, unusual activities, and abandoned packages and to monitor utility supplies and routine work activities scheduled on or near assets.
- Regularly inspect lockers, mail room areas, trash bins, parking lots, garages, and all designated security areas under access control.
- Consider using night vision/infrared CCTVs to monitor areas requiring dim lighting (e.g., theatres, shows, and zoo/aquarium dark habitat facilities).

- **Infrastructure Interdependencies**

- Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, telecommunications).
- Locate fuel and utility supply facilities at a safe distance from buildings and high-traffic areas.



- **Cyber Security**

- Implement and review hardware, software, and communications security for computer-based operational systems.
- Eliminate any information that might provide security information to adversaries from the Web site.

- **Incident Response**

- Develop and maintain an up-to-date emergency response plan.
- Review unified incident command procedure for responding to an event with local law enforcement and emergency responders and government agencies.

- **Report Suspicious Activity**

- If you observe suspicious activity, you should call 911 at once.

Public Assembly – Parades, Festivals, Rallies



Large outdoor public gatherings encompass many disparate events and activities. They include, but are not limited to, parades, fairs, festivals, rallies, flea markets, demonstrations, concerts, and celebrations. Unlike limited-duration events at fixed facilities, large outdoor public gatherings neither require nor rely on a permanent allocation of dedicated security resources. Rather, they usually rely on local law enforcement to provide security during the event. Furthermore, these events normally do not take place in a confined location. Thus, almost all aspects of security must be uniquely planned and formulated for each individual gathering.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to large, outdoor gatherings include:

- Improvised explosive devices
- Arson
- Small arms attack
- Assassination/Kidnapping
- Chemical/biological/radiological agents

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack or that may be associated with terrorist surveillance, training, planning, preparation, or mobilization activities. The observation of any one indicator may not, by itself, suggest terrorist activity. Each observed anomaly or incident, however, should be carefully considered, along with all other relevant observations, to determine whether further investigation is warranted. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the facility of interest and what it might look like. The key factor in early recognition of terrorist activity is the ability to recognize anomalies in location, timing and character of vehicles, equipment, people, and packages.

The potential indicators can be grouped into the following categories:

- *Imminent Attack Indicators.* These indicators may show that an attack is imminent and that immediate action needs to be taken.
- *Surveillance Indicators.* These indicators may provide evidence that a facility or location is under surveillance by terrorists planning an attack.
- *Transactional Indicators.* These indicators stem from unusual business transactions at a facility or location that may indicate that criminal or terrorist activity is being planned.
- *Surrounding Area Indicators.* These indicators relate to activities in the area or region surrounding a facility or location and may demonstrate that an attack is being prepared.

Indicators of potential attack include:

- Persons in crowded areas (e.g., audiences, food service area) wearing unusually bulky clothing that might conceal suicide explosives. Such individuals might be patting down or feeling under their clothing, displaying electrical wires from under their clothing, tightly clutching an object that could be a trigger device, displaying excessive nervousness or anxiety, wearing an excessive amount of cologne or perfume to mask the scent of explosives, or concealing weapons (e.g., automatic rifle) under their clothing.
- Persons or teams of people spotted in or around the gathering and attempting to gain illegal entry (e.g., scaling fences, breaking into doors) or appearing to prepare to launch stand-off weapons (e.g., rocket-propelled grenades) at the gathering.
- Vehicles illegally parked near places where large numbers of people gather. The vehicle may be a car, motorcycle, or truck. The vehicle may be unattended or may have a driver who will detonate it. The driver may demonstrate nervousness and anxiety and may be constantly scanning the area for law enforcement and/or to impact the largest number of victims.

- Unexpected or unfamiliar delivery trucks or service vehicles arriving at the gathering location.
- Vehicles approaching the gathering at unusually high speed and/or steering around barriers and traffic controls.
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives. Packages may be left in open areas or hidden in trash receptacles, lockers, or similar containers.
- Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, security cameras, motion sensors, or other security devices.
- Persons using or carrying video/camera/observation equipment in or near the facility over an extended period.
- Persons discovered with maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel.
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
- Persons questioning gathering sponsor or support personnel off-site about practices pertaining to the event and its operations.

Common Vulnerabilities

The following are key common vulnerabilities of large outdoor gatherings:

- Unrestricted public access
- Temporary structures
- Unrestricted access to peripheral areas, such as parking lots
- Event/activity atmosphere (congestion, noise, disorganization)
- Hostile participants
- Limited employee background checks
- Limited security force
- Lack of exercises for emergency plans
- Multiple locations to place explosives or hazardous agents

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for large outdoor gatherings include:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan
- Conduct regular exercises of the plans
- Maintain constant awareness of current threat condition and available intelligence information
- Develop policies and procedures for dealing with hoaxes and false alarms
- Establish liaison and regular communication with local law enforcement and emergency responders

• Personnel

- Conduct background checks on all employees
- Incorporate security awareness and appropriate response procedures for security situations into mall and mall tenant employee training programs
- Maintain an adequately sized, equipped, and trained security force

• Access Control

- Provide appropriate signs to restrict access to non-public areas
- Identify and control access by all mall and mall tenant employees, vendors, delivery personnel, and contractors
- Install and regularly test electronic access control systems and intrusion detection systems in sensitive areas
- Identify key areas in or adjacent to mall buildings, and prohibit parking in these areas
- Remove any vehicles that have been parked for an unusual length of time

• Barriers

- Provide adequate locks, gates, doors, and other barriers for designated security areas
- Install and inspect blast-resistant trash containers
- Reduce interior glazing or replace it with shatter-proof material
- Introduce traffic barriers and traffic flow calming techniques
- Install active vehicle crash barriers at selected areas to protect buildings and populated areas

• Monitoring, Surveillance, Inspection

- Install closed-circuit television (CCTV) systems, intruder detection systems, and lighting to cover key areas
- Train security personnel to watch for suspicious or unattended vehicles on or near facilities; watch for repeated visitors or outsiders who have no apparent business in non-public areas of the mall; watch for abandoned parcels, suitcases, backpacks, and packages and any unusual activities; and monitor utility supplies and routine work activities scheduled on or near assets
- Regularly inspect lockers, mail room areas, trash bins, parking lots and garages, and all designated security areas under access control

- **Communications**

- Install, maintain, and regularly test the facility security and emergency communications system
- Develop redundancy in the equipment, power supply, and means used to contact security officials
- Communicate threat level information to mall employees and mall tenants
- Take any threatening or malicious telephone call, facsimile, or bomb threat seriously
- Encourage employees and the public to report any situation or suspicious activity that might constitute a threat

- **Cyber Security**

- Implement and review hardware, software, and communications security for computer-based operational systems
- Eliminate any information from venue web site that might provide security information to adversaries

- **Infrastructure Interdependencies**

- Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, telecommunications)
- Locate fuel storage tanks at least 100 feet from all temporary structures and congregation points

- **Report Suspicious Activity**

- If you observe suspicious activity, you should call 911 at once.



Public Assembly – Stadiums and Arenas



Arenas and stadiums range in size from on-campus field houses and high school football stadiums that can accommodate a few hundred people to downtown sports arenas, large indoor/outdoor stadiums, and automobile racetracks that can accommodate over 100,000 spectators. They host many types of events, including sporting events, concerts, religious gatherings, university/high school graduations, political conventions, and circuses. RFK Stadium and Verizon Center are among the largest venues in the District.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to stadiums and arenas include:

- Explosives (e.g., car bomb, suicide bomber)
- Arson (e.g., firebombing, using accelerants)
- Biological/chemical/radiological agents introduced into the facility
- Hostage-taking
- Indiscriminate shooting of patrons

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., facility common areas, food courts) wearing unusually bulky clothing that might conceal suicide explosives or automatic weapons
- Vehicles (e.g., cars, motorcycles, trucks, boats, or aircraft) illegally parked near facility buildings or near places where large numbers of people gather (the larger the vehicle, the greater the quantity of explosives that might be loaded into it)
- Vehicles approaching the facility at unusually high speeds and/or steering around barriers and traffic controls
-

Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives (packages may be left in open areas or may be hidden in trash receptacles, lockers, or similar containers)

Indicators of potential surveillance by terrorists include:

- Persons discovered with facility maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel
- Persons questioning facility employees off site about practices pertaining to the facility and its operations, or an increase in personal e-mails, telephone calls, faxes, or postal mail requesting information about the facility or one of its key assets
- Facility employees using video/camera/observation equipment that is not job-related
- An increase in threats from unidentified sources by telephone, postal mail, or the e-mail system and/or an increase in reports of threats from outside known, reliable sources
- Unfamiliar cleaning crews or other contract workers with passable credentials, or crews or contract workers attempting to access unauthorized areas

Common Vulnerabilities

The following are key common vulnerabilities of stadiums and arenas:

- Large number of people entering facility for events with varying levels of inspection of the items carried in
- Little or no control or inspection of vehicles entering parking areas adjacent to the facility
- Little or no inspection of items carried in by event participants, vendors, contractors, and maintenance and janitorial personnel
- Limited security of facility (e.g., lock downs, patrols, inspections) between events
- Large number of people present at scheduled and publicly announced events, providing easy targets

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for stadiums and arenas include:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan for the facility
- Establish liaison and regular communication with local law enforcement and emergency responders
- Conduct regular exercises with facility employees
- Review available threat information and determine whether events should be cancelled on the basis of this information

• Personnel

- Conduct background checks on all employees (more detailed checks should be conducted on those who will have access to critical assets)
- Maintain an adequately sized, equipped, and trained security force for all events
- Conduct continuous roving security patrols during special events; expand roving/motorized patrols to outer perimeter

• Access Control

- Establish a process for controlling access and egress to the facility; including designated, monitored points of entry
- Establish a buffer zone and perimeter around the facility and a process for controlling access
- Define and secure controlled areas that require extra security
- Control employee and concessionaire identification and access through use of photo identification badges
- Formally identify gathering areas for tail-gate parties and other such gatherings in locations with natural surveillance and access; make informal areas off-limits and subject to automatic scrutiny

• Barriers

- Increase the number of temporary venue barriers and place them to guide the flow of vehicles
- Offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed

• Communication and Notification

- Maintain contact numbers and checklists to follow in the event of a security-related incident
- During events, maintain instantaneous communication capability with local, state, or federal law enforcement and emergency responders

• Monitoring, Surveillance, Inspection

- Ensure that the venue has an intrusion detection system
- Provide video surveillance systems on venue grounds
- At the beginning and end of each event, inspect

interior/exterior of facility

- Require screening of all patrons before they are allowed to enter the facility's perimeter
- Require screening of all employees, concessionaires, event participants, and delivery and emergency service personnel before they are allowed to enter the facility's perimeter for special events
- Check outdoor air intakes of heating, ventilation, and air conditioning (HVAC) systems to ensure that they are protected

• Infrastructure Interdependencies

- Provide 24/7 guard at utility supply points starting 24 hours before a special event until its conclusion
- Ensure that an emergency power source is provided for critical systems
- Ensure that dumpsters are secured and enclosed

• Cyber Security

- Minimize the number of people with authorized access to computer systems
- Increase computer security levels to maximum, if not already in place

• Incident Response

- Ensure that multiple evacuation routes and rallying points are available
- Inspect all available emergency equipment prior to any event to ensure that it will operate during crisis situations
- Assign specific staff members the responsibility of turning off the gas, electricity, water, and alarm systems in the event of an emergency

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Lodging – Hotels, Motels, Conference Centers



In the District of Columbia, there are hundreds of lodging establishments that cater to businesspersons and tourists from around the world. While peak occupancy usually occurs during the summer months, the District maintains a steady stream of visitors and has to provide accommodations to keep up with the demand. Due to the historical and political significance of the District, it is a target for potential terrorist activity. Lodging establishments play a major role in assuring the safety and security of visitors that are not familiar with the culture of the city.



- Evidence of unauthorized access to HVAC areas of a building, such as indications of unusual substances (e.g., unknown powders, droplets, mists) near air intakes

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment in or near the hotel over an extended period
- Persons discovered with hotel maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel
- Persons questioning hotel employees off-site about practices pertaining to the hotel and its operations, or an increase in personal e-mail, telephone, faxes, or postal mail requesting information about the facility or one of its key assets
- Hotel employees inquiring about facility operations, equipment, assets, or security measures about which they should have no job-related interest
- Hotel employees noted as willfully associating with suspicious individuals

Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to hotels include:

- Improvised explosive devices
- Arson
- Small arms attack
- Chemical/biological/radiological agent attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., hotel lobbies, common areas, restaurants) wearing unusually bulky clothing that might conceal suicide explosives
- Vehicles illegally parked near facility buildings or near places where large numbers of people gather
- Unattended packages (e.g., backpack, briefcase, box) that might contain explosives
- Suspicious packages and/or letters received by mail that might contain explosives or chemical/biological/radiological agents

Common Vulnerabilities

The following are key common vulnerabilities of hotels:

- *Unrestricted public access.* Openness to the general public is a feature common to hotels, and it contributes to the facility's vulnerability.
- *Unrestricted access to peripheral areas.* Hotels can be vulnerable to attacks outside their buildings. Most have parking lots and/or parking garages where guests' vehicles have access with little or no screening.
- *Unrestricted access to areas adjacent to buildings.* Most hotels have guest drop-off and pick-up points that are not distant enough to mitigate blasts from explosives in vehicles.
- *Limited employee background checks.* Many hotels, especially smaller ones, hire staff with little or no background checks.
- *Limited security force.* Many hotels have only a small security force.

- *Unprotected HVAC systems.* In some hotels, access to the HVAC systems is not controlled or monitored.
- *Building designs not security oriented.* Many hotel buildings are not designed with security considerations.
- *Multiple locations to place explosives or hazardous agents.* A hotel has numerous locations where an explosives package can be left without being immediately noticed.

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for hotels include:

• Planning and Preparedness

- Designate an employee as security director to address all security-related activities.
- Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis. Develop a comprehensive security and emergency response plan.
- Establish liaison and regular communication with local law enforcement and emergency responders.
- Conduct regular exercises with hotel employees to test security and emergency response plans.

• Personnel

- Conduct background checks on all employees.
- Incorporate security awareness and appropriate response procedures for security situations into employee training programs.
- Maintain an adequately sized, equipped, and trained security force.
- Check guest identification upon check-in. Provide guests with information on how to report suspicious people or activities.

• Access Control

- Define the hotel perimeter and areas within the hotel that require access control for pedestrians and vehicles.
- Issue photo identification badges to all employees. Require that badge be displayed.
- Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees.
- Restrict the storage of luggage to locations away from areas where large numbers of people congregate.

• Barriers

- Install appropriate perimeter barriers and gates. Implement appropriate level of barrier security.
- Install building perimeter barriers (e.g., fences, bollards, decorative flower pots, high curbs, shallow ditches).
- Install barriers to protect doors and windows from small arms fire and explosive blast effects (e.g., blast-resistant and shatter-resistant glass, offset entryways).

- Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from buildings and areas where large numbers of people congregate.

• Communication and Notification

- Install systems that provide communication with all people at the hotel, including employees, security force, emergency response teams, and guests.
- Install systems that provide communication channels with law enforcement and emergency responders.

• Monitoring, Surveillance, Inspection

- Install video surveillance equipment (e.g., closed-circuit television [CCTV], lighting, night-vision equipment).
- Continuously monitor all people, including guests, entering and leaving the facility.
- Consider acquiring luggage-screening equipment for use during high-threat and/or high-profile events.
- Implement quality control inspections on food supply to hotel restaurants and special events.

• Infrastructure Interdependencies

- Ensure that the hotel has adequate utility service capacity to meet normal and emergency needs.
- Ensure that employees are familiar with how to shut off utility services (e.g., electricity, natural gas) in emergency situations.

• Cyber Security

- Develop and implement a security plan for computer and information systems hardware and software.
- Regularly review the hotel's Web site to ensure no sensitive information is provided.

• Incident Response

- Ensure that an adequate number of emergency response personnel are on duty and/or on call at all times.
- Identify alternate rallying points where employees and others at the facility can gather for coordinated evacuation and/or for "head counts" to ensure all have been evacuated.

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Performance Venues – Theaters, Concert Halls, Auditoriums, and Amphitheaters



Performance venues, including theaters, concert halls, auditoriums, and amphitheaters, range in size from small neighborhood movie theaters or community playhouses to facilities that can accommodate thousands of people. In the United States, there are about 6,000 movie theater locations (with more than 35,000 screens). Some theaters and concert halls are on university campuses. All require the same amount of diligence in maintaining the safety and security of the theater-going public.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to performance venues include:

- Improvised explosive devices
- Arson
- Small arms attack
- Assassination/kidnapping

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., theater lobby) wearing unusually bulky clothing that might conceal suicide explosives
- Persons or teams of people spotted in or around the facility and attempting to gain illegal entry (e.g., scaling fences, breaking into doors) or appearing to prepare to launch stand-off weapons (e.g., rocket-propelled grenades) at the facility
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment in or near the facility over an extended period

- Persons discovered with facility maps, photos, or diagrams with critical assets highlighted or notes regarding infrastructure or listing of personnel
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- An increase in threats from unidentified sources by telephone, postal mail, or the e-mail system and/or an increase in reports of threats from outside known, reliable sources
- Evidence of unauthorized access to the HVAC system

Common Vulnerabilities

The following are key common vulnerabilities of performance venues:

- Ready access to theaters, concert halls, auditoriums, and amphitheaters by patrons and service personnel
- Unrestricted access to peripheral areas, such as parking lots, front lobbies, and food courts
- Scheduled and well-publicized performances
- Low lighting during performances, which is conducive to carrying out terrorist activities

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for performance venues include:

- **Planning and Preparedness**
 - Designate an employee as security director to develop, implement, and coordinate all security-related activities.
 - Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis.
 - Review the themes of shows and/or the background and notoriety of performers from the standpoint of drawing attention of terrorists or certain adversarial groups.

- Establish liaison and regular communications with local law enforcement and emergency responders, state and federal law enforcement and terrorism agencies, public health organizations, and industry organizations to enhance information exchange, clarify emergency responses, track threat conditions, and support investigations.
- Institute layers of security measures on the basis of the expected crowd level or audience participation in the performance.
- Conduct regular evacuation drills with facility employees, clearly outlining the evacuation routes and outdoor assembly points.

• **Personnel**

- Conduct background checks on all employees.
- Maintain up-to-date security training with regular refresher courses. Keep records of employee training that has been completed.
- Maintain an adequately sized, equipped, and trained security force.
- Provide security information and evacuation procedures to patrons before each performance. Advise them to be alert to suspicious activity or items and on how to report such incidents.

• **Access Control**

- Define the facility perimeter and areas within the facility that require access control for pedestrians and vehicles.
- Identify a buffer zone extending out from the facility boundary that can be used to further restrict access to the facility when necessary.
- Perform background checks of all performers and their aides beforehand and limit access to only those that have been preapproved for the performance.
- Provide additional security to ticket counters and cash registers at the facility entrance or in the lobby, which are more vulnerable to attacks.

• **Barriers**

- Evaluate and install appropriate perimeter barriers (e.g., fences, berms, concrete walls) and gates around the facility.
- Install alarms and intrusion detection equipment at perimeter barriers.
- Install barriers at HVAC systems (e.g., screens on intakes, filters) to prevent the introduction of chemical, biological, or radiological agents into the building.

• **Communication and Notification**

- Develop a communication and notification plan that covers voice, data, and video transfer of information related to security.
- Provide the ability to record incoming communications (e.g., telephone calls) to identify potential threats.
- Develop a notification protocol that outlines who should be contacted in emergencies.

• **Monitoring, Surveillance, Inspection**

- Evaluate needs and design a monitoring, surveillance, and inspection program that is consistent with facility operations and security requirements.
- Install video surveillance equipment, night-vision cameras, and intrusion detectors.
- Perform security sweeps of the entire facility before each show or performance.

• **Infrastructure Interdependencies**

- Ensure that the facility has adequate utility service capacity to meet normal and emergency needs.

• **Cyber Security**

- Develop and implement a security plan for computer and information systems hardware and software.

• **Incident Response**

- Review unified incident command procedures for responding to an event with local law enforcement, emergency responders, and government agencies.
- Establish procedures for facility evacuation; ensure the evacuation routes are clear of obstruction.

• **Report Suspicious Activity**

- If you observe suspicious activity, you should call 911 at once.

Retail – Shopping Malls, Retail Centers and Districts



The District has many areas for shopping, ranging in size from small open-air neighborhood “strip” shopping centers containing fewer than 10,000 square feet to super-regional malls with more than 1 million square feet. From Union Station to the Shops at Georgetown Park, realty and property management companies must pay utmost attention to ways to keep visitors to their establishments safe and secure.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to shopping malls include:

- Improvised explosive devices
- Arson
- Chemical/biological/radiological agents
- Small arms attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons in crowded areas (e.g., mall common areas, food courts) wearing unusually bulky clothing that might conceal suicide explosives; weapons (e.g., automatic rifle) may also be concealed under their clothing
- Unattended vehicles illegally parked near mall buildings or places where large numbers of patrons gather
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to heating, ventilation, and air conditioning (HVAC) areas; indications of unusual substances near air intakes

Indicators of potential surveillance by terrorists include:

- Persons using or carrying video/camera/observation equipment over an extended period
- Persons discovered with shopping mall maps, photos, or diagrams with facilities highlighted
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- Mall personnel being questioned off-site about practices pertaining to the mall
- Employees changing working behavior or working more irregular hours
- Persons observed or reported to be observing mall receipts or deliveries
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar cleaning crews or other contract workers
- An increase in buildings being left unsecured
- An increase in threats from unidentified sources
- Unusual or unannounced maintenance activities in the vicinity of the mall
- Sudden losses or thefts of guard force equipment

Common Vulnerabilities

The following are key common vulnerabilities of shopping malls:

- Unrestricted public access
- Large number of access points
- Unrestricted access to peripheral areas, such as parking lots
- Unrestricted access to areas adjacent to buildings
- Access by suppliers, vendors, and maintenance workers to nonpublic areas
- Limited employee background checks
- Limited security force
- Lack of exercises for emergency plans

- Unprotected HVAC systems and utility services
- Building designs that are not security oriented
- Multiple locations to place explosives or hazardous agents

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for shopping malls include:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan
- Conduct regular exercises of the plans
- Maintain constant awareness of current threat condition and available intelligence information
- Develop policies and procedures for dealing with hoaxes and false alarms
- Establish liaison and regular communication with local law enforcement and emergency responders

• Personnel

- Conduct background checks on mall employees
- Incorporate security awareness and appropriate response procedures for security situations into mall and mall tenant employee training programs
- Maintain an adequately sized, equipped, and trained security force

• Access Control

- Provide appropriate signs to restrict access to non-public areas
- Identify and control access by all mall and mall tenant employees, vendors, delivery personnel, and contractors
- Install and regularly test electronic access control systems and intrusion detection systems in sensitive areas
- Identify key areas in or adjacent to mall buildings, and prohibit parking in these areas
- Remove any vehicles that have been parked for an unusual length of time

• Barriers

- Provide adequate locks, gates, doors, and other barriers for designated security areas
- Install and inspect blast-resistant trash containers
- Reduce interior glazing or replace it with shatter-proof material
- Introduce traffic barriers and traffic flow calming techniques
- Install active vehicle crash barriers at selected areas to protect buildings and populated areas

• Monitoring, Surveillance, Inspection

- Install closed-circuit television (CCTV) systems, intruder detection systems, and lighting to cover key areas
- Train security personnel to watch for suspicious or unattended vehicles on or near facilities; watch for repeated visitors or outsiders who have no apparent business in non-public areas of the mall; watch for abandoned parcels, suitcases, backpacks, and packages and any unusual activities; and monitor utility supplies and routine work activities scheduled on or near assets
- Regularly inspect lockers, mail room areas, trash bins, parking lots and garages, and all designated security areas under access control

• Communications

- Install, maintain, and regularly test the facility security and emergency communications system
- Develop redundancy in the equipment, power supply, and means used to contact security officials
- Communicate threat level information to mall employees and mall tenants
- Take any threatening or malicious telephone call, facsimile, or bomb threat seriously
- Encourage employees and the public to report any situation or suspicious activity that might constitute a threat

• Cyber Security

- Implement and review hardware, software, and communications security for computer-based operational systems
- Eliminate any information from mall web site that might provide security information to adversaries

• Infrastructure Interdependencies

- Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, telecommunications)
- Locate fuel storage tanks at least 100 feet from all mall buildings and customer congregation points

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Mail and Package Handling Facilities



The Postal and Shipping Sector receives, processes, transports, and distributes billions of letters and parcels annually. It consists of both private and public components. The Postal and Shipping Sector is mainly composed of four large integrated carriers. These carriers, operating 93% of the sector's assets, systems, networks, and functions, are the United States Postal Service (USPS), Federal Express (FedEx), United Parcel Service of America (UPS), and DHL International (DHL). The remainder of the sector consists of smaller firms providing regional and local courier services, other mail services, mail management for corporations, and chartered air delivery services. Although most of the sector is privately owned, there is a major government presence through the USPS.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to mail and package handling facilities include:

- Biological/chemical/radiological attack (e.g. anthrax-laced letter)
- Improvised explosive devices (e.g. package/letter bomb)
- Small arms attack (e.g. disgruntled employee)

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Intimidating, harassing, bullying, belligerent, or other inappropriate, aberrant, bizarre, or aggressive behavior by an employee
- Unusual request concerning the shipment or labeling of goods
- Suspicious package and/or letter received by a carrier that might contain explosives or CBR agents (The packages or mail may have (1) no return address, (2) excessive postage, (3) been sent from outside the United States, (4) indications of liquids/powder leaking from them, or (5) unusual odors.)
- Packaging that is inconsistent with the shipping mode

Indicators of potential surveillance by terrorists include:

- Persons possessing or observed using observation equipment (e.g. cameras, binoculars, night-vision devices) near the facility over an extended period
- Persons discovered with maps, photos, or diagrams with facilities or key facility components highlighted
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation
- Employees changing working behavior or working more irregular hours
- Persons questioning employees off-site about practices pertaining to the mail or package handling facility and its operations
- Persons questioning electric power company employees about the site's electric power supply system
- Unfamiliar service or contract personnel with passable credentials attempting to access unauthorized areas

Common Vulnerabilities

The following are key common vulnerabilities of shopping malls:

- Anonymous mail
- Ease of introducing biological/chemical/explosive agents
- Large number of points of access to the public
- Ease of mail theft
- Large workforce

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for mail and package handling facilities include:

- **Planning and Preparedness**
 - Designate an employee as security director to develop, implement, and coordinate all security-related activities.

- Develop a comprehensive security and emergency response plan. Coordinate the plan with appropriate agencies. Conduct regular exercises of the plan.
- Establish liaison and regular communication with local law enforcement and emergency responders.
- Establish procedures to implement additional protective measures as the threat level increases.

• **Personnel**

- Conduct background checks on all employees
- Incorporate security awareness and response procedures into employee training programs.
- Require contractors, vendors, and employment agencies to vouch for the background and security of their personnel who will work at the facility.

• **Access Control**

- Provide appropriate signs to restrict access to non-public areas
- Install intrusion detection systems in sensitive areas
- Identify a buffer zone extending out from the facility boundary (both land and water areas) that can be used to further restrict access to the facility when necessary. Coordinate with local law enforcement and the U.S. Coast Guard on buffer zone measures.
- Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement.

• **Barriers**

- Provide adequate locks, gates, doors, and other barriers for designated security areas. Inspect barriers routinely for signs of intrusion.
- Install barriers at heating, ventilation, and air-conditioning (HVAC) systems, hatches, and power substations. Routinely patrol these areas.

• **Communication and Notification**

- Install, maintain, and regularly test the facility security and emergency communications system. Ensure functionality and interoperability with local law enforcement.
- Develop redundancy in the equipment, power supply, and means used to contact security officials
- Take any threatening or malicious telephone call, facsimile, or bomb threat seriously
- Encourage employees and the public to report any situation or suspicious activity that might constitute a threat

• **Monitoring, Surveillance, Inspection**

- Install alarms and intrusion detection devices at the site perimeter. Coordinate with law enforcement.
- Monitor the activities of on-site contractors and vendors. Inspect all work before releasing them.
- Continuously monitor vehicles (e.g. cars, trucks, boats, planes) approaching the facility for threat indicators.

• **Infrastructure Interdependencies**

- Ensure that the facility has adequate utility service capacity to meet normal and emergency needs.
- Where practical, provide for redundancy and emergency backup capability.

• **Cyber Security**

- Implement adequate policies and procedures and instill the appropriate culture regarding cyber security.
- Regularly consult with trade organizations, vendors, or specialists about cyber practices and strategies.
- Validate the credentials and work of contractors and vendors given access to technology systems.
- Immediately cancel access for terminated staff.
- Control physical access to critical technologies.

• **Incident Response**

- Develop and maintain an up-to-date emergency response plan, incident notification process, and emergency calling trees that cover all staff.
- Prepare and emergency operations center to coordinate resources and communications during an incident.

• **Report Suspicious Activity**

- If you observe suspicious activity, you should call 911 at once.

Child Care Centers

Child Care Centers (CCC) provide daytime supervision, recreation, and often medical services for children usually from 0-13 years of age. The child care center can be a stand-alone facility or a tenant in a multi-tenant building.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to large residential buildings include:

- Improvised explosive devices or vehicles
- Arson
- Chemical/biological/radiological (CBR) agents
- Small arms attack or suicide bombers
- Kidnapping

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons (employees, guests, contractors, vendors, tenants) in a building wearing unusually bulky clothing that might conceal suicide explosives or weapons (e.g., gun, automatic rifle)
- Unattended vehicles parked illegally or at the parking area or near the building entrance for no apparent reasonable explanation
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to restricted areas, especially the heating, ventilation, and air-conditioning (HVAC) system; indications of unusual substances near air intakes or exhaust

Indicators of potential surveillance by terrorists include:

- Persons discovered with building photos or diagrams with the detailed layout highlighted
- Persons parking, standing, or loitering in the same area for many days with no apparent reasonable explanation
- Persons using or carrying video/camera/observation equipment over an extended period
- Child care center employees or occupants being questioned off site about security practices that pertain to the building or the location of surveillance equipment
- Building employees changing their working behavior or working more irregular hours
- Persons noticed or reported to be observing building security, HVAC system, delivery, or storage areas
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar employees (e.g., cleaning crews) or other contract workers
- Unusual or unannounced repair or maintenance activities near the building
- Sudden losses or thefts of building surveillance equipment

Common Vulnerabilities

The following are key common vulnerabilities of child care centers.

- Inadequate control of access to the building by nonemployees and their vehicles (at exterior doors, doors to adjacent public transit stations, utility tunnels, loading docks, parking garages)
- The design of a building and materials used to construct it, which might enhance the probability that it would be damaged in an attack
- Inadequate protection of the HVAC system
- Inadequate protection of the utility services (electricity, natural gas, water, communications)
- Inadequate emergency response preparations
- Inadequate control of access to sensitive building information

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a child care centers against threats and to mitigate the effects of an attack. Protective measures for child care centers include:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan (for employees, guests, contractors) to prepare for and respond to emergency situations, including malicious or terrorist actions. Include primary caregivers in planning.
- Conduct regular exercises of the plans.
- Maintain a constant awareness of the current threat condition and available intelligence information.
- Develop policies and procedures for dealing with hoaxes and false alarms.

• Personnel

- Conduct background checks on CCC employees (management, service, maintenance, security guards).
- Incorporate security awareness and appropriate response procedures for emergency situations in training programs for building tenants and employees.

• Access Control

- Deny access to any nonresident who displays suspicious behavior.
- Identify and control access by employees, guests, vendors, delivery personnel, and contractors.
- Remove any vehicles that have been parked for an unusual length of time at or near the building.

• Barriers

- Provide adequate locks, doors, and other barriers for designated areas (elevators; HVAC system, storage, delivery, and utility areas; mechanical rooms; roof).
- To the extent practical, minimize the number of places in public areas where an intruder could remain unseen or that could be used to hide weapons.
- Provide adequate exterior lighting, including emergency lighting, where appropriate, to help in detecting suspicious or unusual activity.

• Communications and Notification

- Install, maintain, and regularly test the building security and emergency communications system.
- Communicate information on the threat level to residents, employees, and security force; encourage residents and employees to report any threat or suspicious situation.
- Take any threatening or malicious telephone call, fax, or bomb threat seriously.

• Monitoring, Surveillance, Inspection

- Install closed-circuit television (CCTV) systems, entrance metal detectors (if practical), intruder detection systems, and lights to cover key areas

(entrances; exits; parking lots; hallways; roof; HVAC, utility system, delivery, mail, and storage areas).

- Monitor contractors and delivery personnel while they are on the premises. Restrict the type of personal items that employees, contractors, vendors, and guests can bring to nonpublic areas of the building.
- Train security personnel and employees to watch for suspicious persons and unattended vehicles in or near the building; abandoned parcels, suitcases, backpacks, and packages; and unusual activities; and to monitor all deliveries to the building.
- Regularly inspect and monitor restricted areas, trash bins, utility and storage areas, parking lots, the roof, mechanical rooms, and HVAC systems.

• Infrastructure Interdependencies

- Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, sewer, communications).

• Cyber Security

- Implement and review, if applicable, computer-based operational systems.
- Eliminate any information that might be useful to adversaries from the CCC's website.

• Incident Response

- Maintain an up-to-date emergency response plan.
- Alert appropriate law enforcement and public health authorities to any evidence of tampering with the HVAC system or water or gas supply or of other malicious, criminal, or terrorist activities.

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Nursing Homes

Nursing homes, or Skilled Nursing Facilities, are structures that vary in size from small (less than 50 beds) to large (100+ or high rise) and are characterized by controlled-access lobbies, common areas (e.g., meeting rooms, exercise rooms), on-site parking, and a staff to care for the residents and maintain the common areas and grounds of the building.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to large residential buildings include:

- Improvised explosive devices or vehicles
- Arson
- Chemical/biological/radiological (CBR) agents
- Small arms attack or suicide bombers

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons (employees, guests, contractors, vendors, tenants) in a building wearing unusually bulky clothing that might conceal suicide explosives or weapons (e.g., gun, automatic rifle)
- Unattended vehicles parked illegally or at the parking area or near the building entrance for no apparent reasonable explanation
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to restricted areas, especially the heating, ventilation, and air-conditioning (HVAC) system; indications of unusual substances near air intakes or exhaust

Indicators of potential surveillance by terrorists include:

- Persons discovered with building photos or diagrams with the detailed layout highlighted

- Persons parking, standing, or loitering in the same area for many days with no apparent reasonable explanation
- Persons using or carrying video/camera/observation equipment over an extended period
- Nursing home employees or occupants being questioned off site about security practices that pertain to the building or the location of surveillance equipment
- Building employees changing their working behavior or working more irregular hours
- Persons noticed or reported to be observing building security, HVAC system, delivery, or storage areas
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar employees (e.g., cleaning crews) or other contract workers
- Unusual or unannounced repair or maintenance activities near the building
- Sudden losses or thefts of building surveillance equipment

Common Vulnerabilities

The following are key common vulnerabilities of nursing home buildings.

- Inadequate control of access to the building by nonresidents and their vehicles (at exterior doors, doors to adjacent public transit stations, utility tunnels, loading docks, parking garages)
- The design of a building and materials used to construct it, which might enhance the probability that it would be damaged in an attack
- Inadequate protection of the HVAC system
- Inadequate protection of the utility services (electricity, natural gas, water, communications)
- Inadequate emergency response preparations
- Inadequate control of access to sensitive building information

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a nursing home against threats and to mitigate the effects of an attack. Protective measures for nursing homes include:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan (for tenants, employees, guests, contractors) to prepare for and respond to emergency situations, including malicious or terrorist actions.
- Conduct regular exercises of the plans.
- Maintain a constant awareness of the current threat condition and available intelligence information.
- Develop policies and procedures for dealing with hoaxes and false alarms.

• Personnel

- Conduct background checks on building employees (management, service, maintenance, security guards).
- Incorporate security awareness and appropriate response procedures for emergency situations in training programs for building tenants and employees.

• Access Control

- Deny access to any nonresident who displays suspicious behavior.
- Identify and control access by employees, residents, guests, vendors, delivery personnel, and contractors.
- Remove any vehicles that have been parked for an unusual length of time at or near the building.

• Barriers

- Provide adequate locks, doors, and other barriers for designated areas (elevators; HVAC system, storage, delivery, and utility areas; mechanical rooms; roof).
- To the extent practical, minimize the number of places in public areas where an intruder could remain unseen or that could be used to hide weapons.
- Provide adequate exterior lighting, including emergency lighting, where appropriate, to help in detecting suspicious or unusual activity.

• Communications and Notification

- Install, maintain, and regularly test the building security and emergency communications system.
- Communicate information on the threat level to residents, employees, and security force; encourage residents and employees to report any threat or suspicious situation.
- Take any threatening or malicious telephone call, fax, or bomb threat seriously.

• Monitoring, Surveillance, Inspection

- Install closed-circuit television (CCTV) systems, entrance metal detectors (if practical), intruder detection systems, and lights to cover key areas (entrances; exits; parking lots; hallways; roof; HVAC, utility system, delivery, mail, and storage areas).
- Monitor contractors and delivery personnel while they are on the premises. Restrict the type of personal items that employees, contractors, vendors, and guests can bring to nonpublic areas of the building.
- Train security personnel to watch for suspicious persons and unattended vehicles in or near the building; abandoned parcels, suitcases, backpacks, and packages; and unusual activities; and to monitor all deliveries to the building.
- Regularly inspect and monitor restricted areas, trash bins, utility and storage areas, parking lots, the roof, mechanical rooms, and HVAC systems.

• Infrastructure Interdependencies

- Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, sewer, communications).

• Cyber Security

- Implement and review, if applicable, computer-based operational systems.
- Eliminate any information that might be useful to adversaries from the nursing home's website.

• Incident Response

- Maintain an up-to-date emergency response plan.
- Alert appropriate law enforcement and public health authorities to any evidence of tampering with the HVAC system or water or gas supply or of other malicious, criminal, or terrorist activities.

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Residential Buildings

Large residential, or multifamily, buildings include apartments, condominiums, and cooperatives. These are generally high-rise structures that are characterized by controlled-access lobbies, common areas (e.g., meeting rooms, exercise rooms), on-site parking, and a staff to maintain the common areas and grounds of the building. Even with these characteristics, it is important for residents, along with management companies, to be participants in keeping their areas safe and secure.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to large residential buildings include:

- Improvised explosive devices or vehicles
- Arson
- Chemical/biological/radiological (CBR) agents
- Small arms attack or suicide bombers

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- Persons (employees, guests, contractors, vendors, tenants) in a building wearing unusually bulky clothing that might conceal suicide explosives or weapons (e.g., gun, automatic rifle)
- Unattended vehicles parked illegally or at the parking area or near the building entrance for no apparent reasonable explanation
- Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- Unauthorized access to restricted areas, especially the heating, ventilation, and air-conditioning (HVAC) system; indications of unusual substances near air intakes or exhaust

Indicators of potential surveillance by terrorists include:

- Persons discovered with building photos or diagrams with the detailed layout highlighted
- Persons parking, standing, or loitering in the same area for many days with no apparent reasonable explanation
- Persons using or carrying video/camera/observation equipment over an extended period
- Residential building employees or occupants being questioned off site about security practices that pertain to the building or the location of surveillance equipment
- Building employees changing their working behavior or working more irregular hours
- Persons noticed or reported to be observing building security, HVAC system, delivery, or storage areas
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unfamiliar employees (e.g., cleaning crews) or other contract workers
- Unusual or unannounced repair or maintenance activities near the building
- Sudden losses or thefts of building surveillance equipment

Common Vulnerabilities

The following are key common vulnerabilities of large residential buildings.

- Inadequate control of access to the building by non-tenants and their vehicles (at exterior doors, doors to adjacent public transit stations, utility tunnels, loading docks, parking garages)
- The design of a building and materials used to construct it, which might enhance the probability that it would be damaged in an attack
- Inadequate protection of the HVAC system
- Inadequate protection of the utility services (electricity, natural gas, water, communications)
- Inadequate emergency response preparations
- Inadequate control of access to sensitive building information

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a residential building against threats and to mitigate the effects of an attack. Protective measures for large residential buildings include:

• Planning and Preparedness

- Develop a comprehensive security plan and emergency response plan (for tenants, employees, guests, contractors) to prepare for and respond to emergency situations, including malicious or terrorist actions.
- Conduct regular exercises of the plans.
- Maintain a constant awareness of the current threat condition and available intelligence information.
- Develop policies and procedures for dealing with hoaxes and false alarms.

• Personnel

- Conduct background checks on building employees (management, service, maintenance, security guards).
- Incorporate security awareness and appropriate response procedures for emergency situations in training programs for building tenants and employees.

• Access Control

- Deny access to any non-tenant who displays suspicious behavior.
- Identify and control access by employees, tenants, guests, vendors, delivery personnel, and contractors.
- Remove any vehicles that have been parked for an unusual length of time at or near the building.

• Barriers

- Provide adequate locks, doors, and other barriers for designated areas (elevators; HVAC system, storage, delivery, and utility areas; mechanical rooms; roof).
- To the extent practical, minimize the number of places in public areas where an intruder could remain unseen or that could be used to hide weapons.
- Provide adequate exterior lighting, including emergency lighting, where appropriate, to help in detecting suspicious or unusual activity.

• Communications and Notification

- Install, maintain, and regularly test the building security and emergency communications system.
- Communicate information on the threat level to tenants, employees, and security force; encourage tenants and employees to report any threat or suspicious situation.
- Take any threatening or malicious telephone call, fax, or bomb threat seriously.

• Monitoring, Surveillance, Inspection

- Install closed-circuit television (CCTV) systems, entrance metal detectors (if practical), intruder detection systems, and lights to cover key areas (entrances; exits; parking lots; hallways; roof; HVAC, utility system, delivery, mail, and storage areas).
- Monitor contractors and delivery personnel while they are on the premises. Restrict the type of personal items that employees, contractors, vendors, and guests can bring to nonpublic areas of the building.
- Train security personnel to watch for suspicious persons and unattended vehicles in or near the building; abandoned parcels, suitcases, backpacks, and packages; and unusual activities; and to monitor all deliveries to the building.
- Regularly inspect and monitor restricted areas, trash bins, utility and storage areas, parking lots, the roof, mechanical rooms, and HVAC systems.

• Infrastructure Interdependencies

- Provide adequate security and backup for critical utility services (e.g., electricity, natural gas, water, sewer, communications).

• Cyber Security

- Implement and review, if applicable, computer-based operational systems.
- Eliminate any information that might be useful to adversaries from the building Web site.

• Incident Response

- Maintain an up-to-date emergency response plan.
- Alert appropriate law enforcement and public health authorities to any evidence of tampering with the HVAC system or water or gas supply or of other malicious, criminal, or terrorist activities.

• Report Suspicious Activity

- If you observe suspicious activity, you should call 911 at once.

Active Shooter: How to Respond



PROFILE OF AN ACTIVE SHOOTER¹

An Active Shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims.

Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims.

Active shooter situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation.

Good practices for coping with an active shooter situation

- Be aware of your environment and any possible dangers
- Take note of the two nearest exits in any facility you visit
- If you are in an office, stay there and secure the door
- If you are in a hallway, get into a room and secure the door
- As a last resort, attempt to take the active shooter down. When the shooter is at close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her.

**CALL 911
WHEN IT IS SAFE TO DO SO!**

¹ *Active Shooter: How to Respond* (Oct 2008). Published in partnership with the Department of Homeland Security; National Tactical Officers Association; Fairfax County, VA Police Department; the National Retail Federation, and the Retail Industry Leaders Association

HOW TO RESPOND WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

Quickly determine the most reasonable way to protect your own life. Remember that customers and clients are likely to follow the lead of employees and managers during an active shooter situation.

1. Evacuate

If there is an accessible escape path, attempt to evacuate the premises. Be sure to:

- Have an escape route and plan in mind
- Evacuate regardless of whether others agree to follow
- Leave your belongings behind
- Help others escape, if possible
- Prevent individuals from entering an area where the active shooter may be
- Keep your hands visible
- Follow the instructions of any police officers
- Do not attempt to move wounded people
- Call 911 when you are safe

2. Hide out

If evacuation is not possible, find a place to hide where the active shooter is less likely to find you.

Your hiding place should:

- Be out of the active shooter's view
- Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
- Not trap you or restrict your options for movement

To prevent an active shooter from entering your hiding place:

- Lock the door
- Blockade the door with heavy furniture

If the active shooter is nearby:

- Lock the door
- Silence your cell phone and/or pager
- Turn off any source of noise (i.e., radios, televisions)
- Hide behind large items (i.e., cabinets, desks)
- Remain quiet

If evacuation and hiding out are not possible:

- Remain calm
- Dial 911, if possible, to alert police to the active shooter's location
- If you cannot speak, leave the line open and allow the dispatcher to listen

3. Take action against the active shooter

As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:

- Acting as aggressively as possible against him/her
- Throwing items and improvising weapons
- Yelling
- Committing to your actions

HOW TO RESPOND WHEN LAW ENFORCEMENT ARRIVES

Law enforcement's purpose is to stop the active shooter as soon as possible. Officers will proceed directly to the area in which the last shots were heard.

- Officers usually arrive in teams of four (4)
- Officers may wear regular patrol uniforms or external bulletproof vests, Kevlar helmets, and other tactical equipment
- Officers may be armed with rifles, shotguns, handguns
- Officers may use pepper spray or tear gas to control the situation
- Officers may shout commands, and may push individuals to the ground for their safety

How to react when law enforcement arrives:

- Remain calm, and follow officers' instructions
- Put down any items in your hands (i.e., bags, jackets)
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as holding on to them for safety
- Avoid pointing, screaming and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

Information to provide to law enforcement or 911 operator:

- Location of the active shooter
- Number of shooters, if more than one

- Physical description of shooter/s
- Number and type of weapons held by the shooter/s
- Number of potential victims at the location

The first officers to arrive to the scene will not stop to help injured persons. Expect rescue teams comprised of additional officers and emergency medical personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

Once you have reached a safe location or an assembly point, you will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave until law enforcement authorities have instructed you to do so.

TRAINING YOUR STAFF FOR AN ACTIVE SHOOTER SITUATION

To best prepare your staff for an active shooter situation, create an Emergency Action Plan (EAP), and conduct training exercises. Together, the EAP and training exercises will prepare your staff to effectively respond and help minimize loss of life.

Components of an Emergency Action Plan (EAP) Create the EAP with input from several stakeholders including your human resources department, your training department (if one exists), facility owners/operators, your property manager, and local law enforcement and/or emergency responders. **An effective EAP includes:**

- A preferred method for reporting fires and other emergencies
- An evacuation policy and procedure
- Emergency escape procedures and route assignments (i.e., floor plans, safe areas)
- Contact information for, and responsibilities of individuals to be contacted under the EAP
- Information concerning local area hospitals (i.e., name, telephone number, and distance from your location)
- An emergency notification system to alert various parties of an emergency including:
 - Individuals at remote locations within premises
 - Local law enforcement
 - Local area hospitals

Components of Training Exercises

The most effective way to train your staff to respond to an active shooter situation is to conduct mock active shooter training exercises. Local law enforcement is an excellent resource in designing training exercises.

- Recognizing the sound of gunshots
- Reacting quickly when gunshots are heard and/or when a shooting is witnessed:
 - Evacuating the area
 - Hiding out
 - Acting against the shooter as a last resort
- Calling 911
- Reacting when law enforcement arrives

- Adopting the survival mind set during times of crisis

Additional Ways to Prepare For and Prevent an Active Shooter Situation

- Preparedness
 - Ensure that your facility has at least two evacuation routes
 - Post evacuation routes in conspicuous locations throughout your facility
 - Include local law enforcement and first responders during training exercises
 - Encourage law enforcement, emergency responders, SWAT teams, K-9 teams and bomb squads to train for an active shooter scenario at your location
- Prevention
 - Foster a respectful workplace
 - Be aware of indications of workplace violence and take remedial actions accordingly

PREPARING FOR AND MANAGING AN ACTIVE SHOOTER SITUATION

Your human resources department and facility managers should engage in planning for emergency situations, including an active shooter scenario. Planning for emergency situations will help to mitigate the likelihood of an incident by establishing the mechanisms described below.

Human Resources' Responsibilities

- Conduct effective employee screening and background checks
- Create a system for reporting signs of potentially violent behavior
- Make counseling services available to employees
- Develop an Emergency Action Plan which includes policies and procedures for dealing with an active shooter situation, as well as after action planning

Facility Manager Responsibilities

- Institute access controls (i.e., keys, security system pass codes)
- Distribute critical items to appropriate managers / employees, including:
 - Floor plans
 - Keys
 - Facility personnel lists and telephone numbers
- Coordinate with the facility's security department to ensure the physical security of the location

Assemble crisis kits containing:

- radios
- floor plans
- staff roster, and staff emergency contact numbers
- first aid kits
- flashlights
- Place removable floor plans near entrances and exits for emergency responders
- Activate the emergency notification system when an emergency situation occurs

Reactions of Managers During an Active Shooter Situation

Employees and customers are likely to follow the lead of managers during an emergency situation. During an emergency, managers should be familiar with their EAP, and be prepared to:

- Take immediate action
- Remain calm
- Lock and barricade doors
- Evacuate staff and customers via a preplanned evacuation route to a safe area assisting individuals with special needs and/or disabilities
- Ensure that EAPs, evacuation instructions and any other relevant information address to individuals with special needs and/or disabilities
- Identify options to address individuals with limited English proficiencyⁱ
- Your building should be handicap-accessible, in compliance with ADA requirements

RECOGNIZING POTENTIAL WORKPLACE VIOLENCE

An active shooter in your workplace may be a current or former employee, or an acquaintance of a current or former employee. Intuitive managers and coworkers may notice characteristics of potentially violent behavior in an employee. Alert your Human Resources Department if you believe an employee or coworker exhibits potentially violent behavior.

Indicators of Potential Violence by an Employee

Employees typically do not just “snap,” but display indicators of potentially violent behavior over time. If these behaviors are recognized, they can often be managed and treated. Potentially violent behaviors by an employee may include one or more of the following (this list of behaviors is not comprehensive, nor is it intended as a mechanism for diagnosing violent tendencies):

- Increased use of alcohol and/or illegal drugs
- Unexplained increase in absenteeism; vague physical complaints
- Noticeable decrease in attention to appearance and hygiene
- Depression / withdrawal
- Resistance and overreaction to changes in policy and procedures
- Repeated violations of company policies
- Increased severe mood swings
- Noticeably unstable, emotional responses
- Explosive outbursts of anger or rage without provocation
- Suicidal; comments about “putting things in order”
- Behavior which is suspect of paranoia, (“everybody is against me”)
- Increasingly talks of problems at home
- Escalation of domestic problems into the workplace; talk of severe financial problems
- Talk of previous incidents of violence
- Empathy with individuals committing violence
- Increase in unsolicited comments about firearms, other dangerous weapons and violent crimes

MANAGING THE CONSEQUENCES OF AN ACTIVE SHOOTER SITUATION

After the active shooter has been incapacitated and is no longer a threat, human resources and/or management should engage in post-event assessments and activities, including:

- An accounting of all individuals at a designated assembly point to determine who, if anyone, is missing and potentially injured

- Determining a method for notifying families of individuals affected by the active shooter, including notification of any casualties
- Assessing the psychological state of individuals at the scene, and referring them to health care specialists accordingly
- Identifying and filling any critical personnel or operational gaps left in the organization as a result of the active shooter

LESSONS LEARNED

To facilitate effective planning for future emergencies, it is important to analyze the recent active shooter situation and create an after action report. The analysis and reporting contained in this report is useful for:

- Serving as documentation for response activities
- Identifying successes and failures that occurred during the event
- Providing an analysis of the effectiveness of the existing EAP
- Describing and defining a plan for making improvements to the EAP

References

Safety Guidelines for Armed Subjects, Active Shooter Situations, Indiana University Police Department, April 2007.
Safety Tips & Guidelines Regarding Potential “Active Shooter” Incidents Occurring on Campus, University of California Police.
Shots Fired, When Lightning Strikes (DVD), Center for Personal Protection and Safety, 2007.
Workplace Violence Desk Reference, Security Management Group International, www.SMGICorp.com
How to Plan for Workplace Emergencies and Evacuations, U.S. Department of Labor, Occupational Health and Safety Administration, OSHA 3088, 2001.

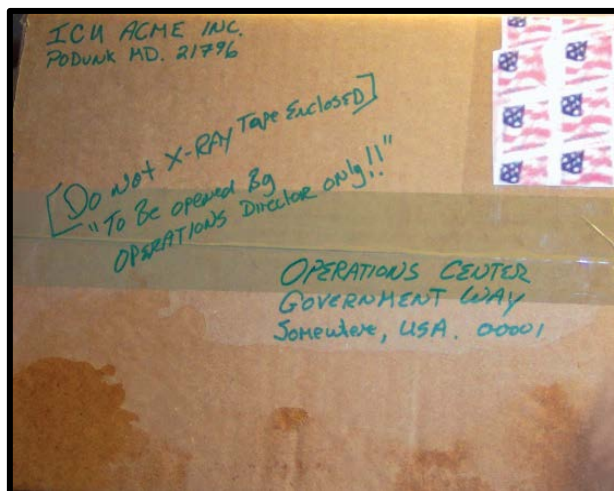
Response Checklist: Suspicious Packages and Mail



CHARACTERISTICS OF A SUSPICIOUS PACKAGEⁱⁱ

Always Remain Aware and Look for the Anomalies:

- Rigid or bulky
- Lopsided or uneven
- Wrapped in string
- Badly written or misspelled labels
- Foreign writing, postage, or return address
- Missing, nonsensical, or unknown return address
- Leaks, stains, powders, or protruding materials
- Ticking, vibration, or other sound
- No postage
- Generic or incorrect titles
- Excessive postage



Call 9-1-1 to Report Suspicious Packages

CHECKLIST OF ACTIONS TO TAKE

Step 1

Leave the mail piece or substance where it was found. Do not disturb. Do not try to clean up the substance

Step 2

Clear the immediate area of all persons and keep others away

Step 3

Instruct people in the immediate area to wash hands and other exposed skin with soap and water

Step 4

Direct these people to a designated area away from the substance to await further instruction

Step 5

List the names of the persons in the immediate area of the mail piece or substance

Step 6

Cordon off the immediate area

Step 7

Shut down all equipment in the immediate area and HVAC systems (heating, ventilation, and air conditioning)

Step 8

If possible without disturbing the mail piece or substance, document:

- Location of mail piece or substance
- Description of substance
- Description of mail piece (markings, labels, declarations, postage)
- Addressee's name and address
- Mailer's name and address

Step 9

District residents, businesses, and visitors should **contact 9-1-1** and pass information documented in Step 8









Step 10

Take actions and make appropriate notifications as directed or as published in your local emergency plan

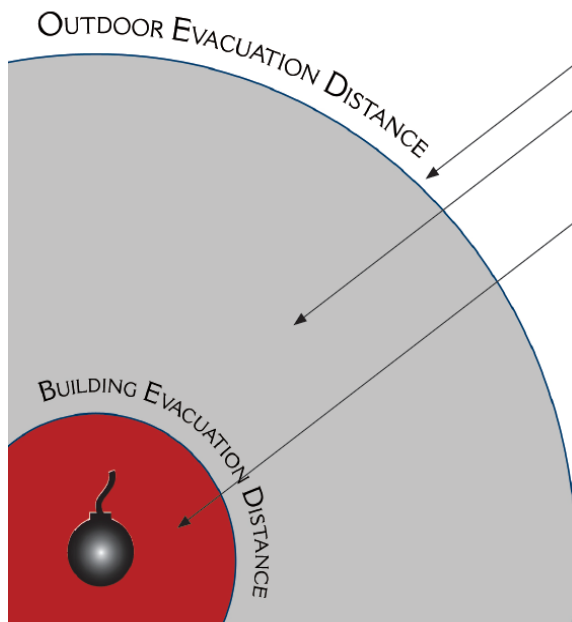


Bomb Threat: Stand-Off Chart

It is important to note that the given distances do not guarantee safety, they are estimates based on test data and the area near and around the evacuation distances are still potentially dangerous. Minimum evacuation distance is the range at which a life-threatening injury from blast or fragmentation hazards is unlikely. However, non-life-threatening injury or temporary hearing loss may occur.ⁱⁱⁱ

Threat Description Improvised Explosive Device (IED)	Explosives Capacity ¹ (TNT Equivalent)	Building Evacuation Distance ²	Outdoor Evacuation Distance ³
 Pipe Bomb	5 LBS	70 FT	1200 FT
 Suicide Bomber	20 LBS	110 FT	1700 FT
 Briefcase/Suitcase	50 LBS	150 FT	1850 FT
 Car	500 LBS	320 FT	1500 FT
 SUV/Van	1,000 LBS	400 FT	2400 FT
 Small Moving Van/ Delivery Truck	4,000 LBS	640 FT	3800 FT
 Moving Van/ Water Truck	10,000 LBS	860 FT	5100 FT
 Semi-Trailer	60,000 LBS	1570 FT	9300 FT

1. These capacities are based on the maximum weight of explosive material that could reasonably fit in a container of similar size.
2. Personnel in buildings are provided a high degree of protection from death or serious injury; however, glass breakage and building debris may still cause some injuries. Un-strengthened buildings can be expected to sustain damage that approximates five percent of their replacement cost.
3. If personnel cannot enter a building to seek shelter they must evacuate to the minimum distance recommended by Outdoor Evacuation Distance. These distances are governed by the greater hazard of fragmentation distance, glass breakage or threshold for ear drum rupture.



Preferred area (beyond this line) for evacuation of people in buildings and mandatory for people outdoors.

All personnel in this area should seek shelter immediately inside a building away from windows and exterior walls. Avoid having anyone outside - including those evacuating - in this area.

All personnel must evacuate (both inside of buildings and out).

1. Based on maximum volume or weight of explosive (TNT equivalent) that could reasonably fit in a suitcase or vehicle.
2. Governed by the ability of typical US commercial construction to resist severe damage or collapse following a blast. Performance can vary significantly, however, and buildings should be analyzed by qualified parties when possible.
3. Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges that throw fragments farther than vehicle bombs.
4. A known terrorist tactic is to attract bystanders to windows, doorways, and the outside with gunfire, small bombs, or other methods and then detonate a larger, more destructive device, significantly increasing human casualties.

Bomb Threat: Telephonic Response Checklist



Your Name:	Date:
Time Call Received:	Ended:

ASK:

1. Where is the bomb now?
2. When is the bomb going to explode?
3. What kind of bomb is it?
4. What does the bomb look like?
5. Who placed the bomb?
6. Why was the bomb placed there?
7. Obtain full name and address of informants

- | | | |
|----------------------------------|------------------------------------|--|
| <input type="checkbox"/> Calm | <input type="checkbox"/> Laughter | <input type="checkbox"/> Angry |
| <input type="checkbox"/> Excited | <input type="checkbox"/> Distinct | <input type="checkbox"/> Crying |
| <input type="checkbox"/> Slow | <input type="checkbox"/> Slurred | <input type="checkbox"/> Deep |
| <input type="checkbox"/> Rapid | <input type="checkbox"/> Nasal | <input type="checkbox"/> Ragged |
| <input type="checkbox"/> Soft | <input type="checkbox"/> Stutter | <input type="checkbox"/> Clearing throat |
| <input type="checkbox"/> Loud | <input type="checkbox"/> Lisp | <input type="checkbox"/> Deep breathing |
| <input type="checkbox"/> Normal | <input type="checkbox"/> Raspy | <input type="checkbox"/> Cracking voice |
| <input type="checkbox"/> Accent | <input type="checkbox"/> Disguised | <input type="checkbox"/> Familiar |

If the voice is familiar, who did it sound like?

- ☐ Well spoken (educated)
- ☐ Foul
- ☐ Irrational
- ☐ Foreign accent (language)
- ☐ Incoherent
- ☐ Taped
- ☐ Message sounded read

BACKGROUND SOUNDS:

- | | |
|---|--|
| <input type="checkbox"/> Street Noises | <input type="checkbox"/> Factory noises |
| <input type="checkbox"/> Television | <input type="checkbox"/> Animal noises |
| <input type="checkbox"/> Voices | <input type="checkbox"/> Clear |
| <input type="checkbox"/> PA System | <input type="checkbox"/> Static |
| <input type="checkbox"/> Music | <input type="checkbox"/> Local |
| <input type="checkbox"/> House noises | <input type="checkbox"/> Long distance |
| <input type="checkbox"/> Motor noises | <input type="checkbox"/> Telephone booth |
| <input type="checkbox"/> Office machinery | <input type="checkbox"/> Other _____ |
| <input type="checkbox"/> Traffic noises | _____ |
| <input type="checkbox"/> Air traffic noises | _____ |

EXACT WORDS OF PERSON PLACING THE CALL:

SEX:

- ☐ Male
- ☐ Female

Approximate Age:

REPORT CALL IMMEDIATELY TO:

- ☐ 911
- ☐ Your supervisor or anyone in management
- ☐ The Emergency Action Coordinator for your building

Shelter-in-Place Facts and Checklist:

Residential



What Shelter-in-Place Means:

One of the instructions you may be given in an emergency where hazardous materials may have been released into the atmosphere is to shelter-in-place. This is a precaution aimed to keep you safe while remaining indoors. (This is not the same thing as going to a shelter in case of a storm.) Shelter-in-place means selecting a small, interior room, with no or few windows, and taking refuge there. It does not mean sealing off your entire home or office building. If you are told to shelter-in-place, follow the instructions provided in this Fact Sheet.

Why You Might Need to Shelter-in-Place:

Chemical, biological, or radiological contaminants may be released accidentally or intentionally into the environment. Should this occur, information will be provided by local authorities on television and radio stations on how to protect you and your family. Because information will most likely be provided on television and radio, it is important to keep a TV or radio on, even during the workday. The important thing is for you to follow instructions of local authorities and know what to do if they advise you to shelter-in-place.

How to Shelter-in-Place

At Home:

- Close and lock all windows and exterior doors.
- If you are told there is danger of explosion, close the window shades, blinds, or curtains.
- Turn off all fans, heating and air conditioning systems.
- Close the fireplace damper.
- Get your family disaster supplies kit <http://www.redcross.org/services/disaster/beprepared/supplies.html>, and make sure the radio is working.
- Go to an interior room without windows that's above ground level. In the case of a chemical threat, an above-ground location is preferable because some chemicals are heavier than air, and may seep into basements even if the windows are closed.
- Bring your pets with you, and be sure to bring additional food and water supplies for them.
- It is ideal to have a hard-wired telephone in the room you select. Call your emergency contact and have the phone available if you need to report a life-threatening condition. Cellular telephone equipment may be overwhelmed or damaged during an emergency.
- Use duct tape and plastic sheeting (heavier than food wrap) to seal all cracks around the door and any vents into the room.
- Keep listening to your radio or television until you are told all is safe or you are told to evacuate. Local officials may call for evacuation in specific areas at greatest risk in your community.

At Work:

- Close the business.
- Bring everyone into the room(s). Close and lock the door(s).
- If there are customers, clients, or visitors in the building, provide for their safety by asking them to stay – not leave. When authorities provide directions to shelter-in-place, they want everyone to take those steps now, where they are, and not drive or walk outdoors.
- Unless there is an imminent threat, ask employees, customers, clients, and visitors to call their emergency contact to let them know where they are and that they are safe.
- Turn on call-forwarding or alternative telephone answering systems or services. If the business has voice mail or an automated attendant, change the recording to indicate that the business is closed, and that staff and visitors are remaining in the building until authorities advise it is safe to leave.
- Close and lock all windows, exterior doors, and any other openings to the outside.
- If you are told there is danger of explosion, close the window shades, blinds, or curtains.

- Have employees familiar with your building's mechanical systems turn off all fans, heating and air conditioning systems.
- Some systems automatically provide for exchange of inside air with outside air – these systems, in particular, need to be turned off, sealed, or disabled.
- Gather essential disaster supplies, such as nonperishable food, bottled water, battery-powered radios, first aid supplies, flashlights, batteries, plastic sheeting, and plastic garbage bags.
- Select interior room(s) above the ground floor, with the fewest windows or vents. The room(s) should have adequate space for everyone to be able to sit in. Avoid overcrowding by selecting several rooms if necessary. Large storage closets, utility rooms, pantries, copy and conference rooms without exterior windows will work well. Avoid selecting a room with mechanical equipment like ventilation blowers or pipes, because this equipment may not be able to be sealed from the outdoors.
- It is ideal to have a hard-wired telephone in the room(s) you select. Call emergency contacts and have the phone available if you need to report a life-threatening condition. Cellular telephone equipment may be overwhelmed or damaged during an emergency.
- Write down the names of everyone in the room, and call your business' designated emergency contact to report who is in the room with you, and their affiliation with your business (employee, visitor, client, customer.)
- Keep listening to the radio or television until you are told all is safe or you are told to evacuate. Local officials may call for evacuation in specific areas at greatest risk in your community.

At School:

- Close the school. Activate the school's emergency plan. Follow reverse evacuation procedures to bring students, faculty, and staff indoors.
- If there are visitors in the building, provide for their safety by asking them to stay – not leave. When authorities provide directions to shelter-in-place, they want everyone to take those steps now, where they are, and not drive or walk outdoors.
- Provide for answering telephone inquiries from concerned parents by having at least one telephone with the school's listed telephone number available in the room selected to provide shelter for the school secretary, or person designated to answer these calls. This room should also be sealed. There should be a way to communicate among all rooms where people are sheltering-in-place in the school.
- Ideally, provide for a way to make announcements over the school-wide public address system from the room where the top school official takes shelter.
- If children have cell phones, allow them to use them to call a parent or guardian to let them know that they have been asked to remain in school until further notice, and that they are safe.
- If the school has voice mail or an automated attendant, change the recording to indicate that the school is closed, students and staff are remaining in the building until authorities advise that it is safe to leave.
- Provide directions to close and lock all windows, exterior doors, and any other openings to the outside.
- If you are told there is danger of explosion, direct that window shades, blinds, or curtains be closed.
- Have employees familiar with your building's mechanical systems turn off all fans, heating and air conditioning systems. Some systems automatically provide for exchange of inside air with outside air – these systems, in particular, need to be turned off, sealed, or disabled.
- Gather essential disaster supplies, such as nonperishable food, bottled water, battery-powered radios, first aid supplies, flashlights, batteries, plastic sheeting, and plastic garbage bags.
- Select interior room(s) above the ground floor, with the fewest windows or vents. The room(s) should have adequate space for everyone to be able to sit in. Avoid overcrowding by selecting several rooms if necessary. Classrooms may be used if there are no windows or the windows are sealed and cannot be opened. Large storage closets, utility rooms, meeting rooms, and even a gymnasium without exterior windows will also work well.
- It is ideal to have a hard-wired telephone in the room(s) you select. Call emergency contacts and have the phone available if you need to report a life-threatening condition. Cellular telephone equipment may be overwhelmed or damaged during an emergency.
- Bring everyone into the room. Shut and lock the door.
- Use duct tape and plastic sheeting (heavier than food wrap) to seal all cracks around the door(s) and any vents into the room.
- Write down the names of everyone in the room, and call your schools' designated emergency contact to report who is in the room with you.

- Listen for an official announcement from school officials via the public address system, and stay where you are until you are told all is safe or you are told to evacuate. Local officials may call for evacuation in specific areas at greatest risk in your community.

In Your Vehicle:

If you are driving a vehicle and hear advice to “shelter-in-place” on the radio, take these steps:

- If you are very close to home, your office, or a public building, go there immediately and go inside. Follow the shelter-in-place recommendations for the place you pick described above.
- If you are unable to get to a home or building quickly and safely, then pull over to the side of the road. Stop your vehicle in the safest place possible. If it is sunny outside, it is preferable to stop under a bridge or in a shady spot, to avoid being overheated.
- Turn off the engine. Close windows and vents.
- If possible, seal the heating/air conditioning vents.
- Listen to the radio regularly for updated advice and instructions.
- Stay where you are until you are told it is safe to get back on the road. Be aware that some roads may be closed or traffic detoured. Follow the directions of law enforcement officials.

Local officials on the scene are the best source of information for your particular situation. Following their instructions during and after emergencies regarding sheltering, food, water, and cleanup methods is your safest choice.

Remember that instructions to shelter-in-place are usually provided for durations of a few hours, not days or weeks. There is little danger that the room in which you are taking shelter will run out of oxygen and you will suffocate.

Sheltering in place in your workplace is similar to sheltering in place at home, but there are some significant differences.^{iv}

The basic steps remain the same:

1. Shut and lock all windows and doors
2. Turn off all air handling equipment (heating, ventilation, and/or air conditioning)
3. Go to a pre-determined sheltering room (or rooms)
4. Seal any windows and/or vents where possible
5. Seal the door(s) with duct tape around the top, bottom and sides
6. Turn on a TV or radio and listen for further instructions.
7. When the “all clear” is announced, open windows and doors, turn on ventilation systems and go outside until the building’s air has been exchanged with the now clean outdoor air.

Additional steps that offices need to consider:

1. Employees cannot be forced to shelter in place. Therefore, it is important to develop your shelter in place plan with employees to maximize the cooperation of employees with the shelter plan. Determine if all employees will shelter or if some will leave the building before shelter procedures are put in place.
2. Develop an accountability system. You should know who is in your building and where they are if an emergency develops. Visitors should be made aware of your office’s decision to shelter in place if advised by emergency management officials.
3. Duties should be assigned to specific employees. Those employees should have backups.
4. Drills should be planned and executed on a regular basis. Afterwards, the drill should be critiqued by employees and/or drill monitors from the local emergency management agency. Lessons learned should be incorporated into your Shelter in Place plan.

Before an emergency occurs:

Discuss emergency procedures with all employees. Explain sheltering in place to your employees or invite the LEPC or local Fire Chief to explain the emergency warning system and sheltering in place. By having a discussion with all employees about sheltering in place and its use, the team approach can work to implement an effective sheltering plan.

Select a room or rooms to serve as shelter rooms during chemical emergencies. The rooms should be large enough to provide at least 10 square feet per person sheltered. A shelter room should have as few windows, vents and doors as possible. A windowless room is best. The LEPC or Fire Chief can provide assistance in selecting the best room(s) for sheltering.

Break rooms or conference rooms with few or no windows can be used for shelters. Hallways are sometimes used in institutional settings. In a closet or other storage area in the shelter room, supplies for sheltering should be stored.

Before a chemical accident occurs, outfit your shelter kit with the following:

- Plastic sheeting - Pre-cut plastic sheeting to fit over any windows or vents in the sheltering area.
- Battery operated radio with fresh batteries - In the event of a power outage, a battery operated radio is necessary to hear emergency announcements including the “all clear” when the emergency is over.
- Flashlight and fresh batteries.
- Bottled water for drinking.
- First aid kit

The shelter room should also have a telephone (either regular or cellular) for emergency use only. Stay off the phone during the shelter in place to keep lines free for emergency responders. If you have an emergency in your shelter room, use the phone to call 911 for help.

Check your shelter kit on a regular basis. Supplies can sometimes disappear when all employees know where the shelter kit is stored. Batteries for the radio and flashlight should be kept fresh.

Develop an emergency plan and checklist with your employees. Volunteers or recruits should be assigned specific duties during an emergency. Alternates should be assigned to each duty.

Plan at least two shelter in place drills annually. The first drill can be announced, and then later drills should be unannounced. It is useful to invite outside drill monitors to observe your drill and to participate in an after-drill critique. Critiques can provide you with valuable insights to improve protection for you and your employees during chemical emergencies.

Modify the Shelter in Place plan to suit your particular situation. Please refer to the next page.

SAMPLE PLAN

This is an example of a plan that a business could develop for shelter in place actions. You should develop your own plan with an employee planning team. The following plan can be used to assist in developing your own plan.

Shelter In Place Plan for ABC Company, Inc.

1234 Jones Boulevard
Anywhere, USA

NOTICE!

In the event that a shelter in place is advised for the area including the ABC Company, all persons in the building will be notified that ABC Company is preparing to shelter in place and that all doors will be locked after 3 minutes. All employees and visitors must decide whether to shelter in place at ABC Company until the “all clear” is announced or whether they will leave the premises within 3 minutes. After that time, no one will be allowed to break the seal on the building until the “all clear” is announced.

Shelter In Place Procedures

Communications:

<u>Procedure</u>	<u>Responsible Party</u>	<u>Needed Supplies/ Equipment/Rules</u>
Listen for announcement on radio/weather radio/TV	receptionist	weather radio
Announce to employees and visitors that a shelter in place has been advised and that the sheltering plan should be implemented immediately	receptionist	intercom system
Locate cellular phone (take to the break room)	receptionist	cell phones in sales office, executive suite
Take employee and visitor sign-in sheets to the shelter area (break room)	receptionist	All employees and visitors must sign in and out of the building at the reception desk

Control of air movement:

<u>Procedure</u>	<u>Responsible Party</u>	<u>Needed Supplies/ Equipment/Rules</u>
When intercom announces shelter in place, immediately turn off all air handling equipment	Maintenance Dept. 1) Chief of Maintenance 2) Maintenance Supervisor	Locate main cutoff switch for heating, cooling and ventilation systems. Label with shelter in place shutoff
Make sure all windows are closed and locked	Each office inhabitant must assure that his/her windows are closed and locked. Floor monitor/ alternate checks offices, windows (in offices and in common areas) and closes office doors as he/she moves to shelter room. Make sure all fire doors are closed.	
When 3 minutes have elapsed, place sign on outside and lock all outside doors	Janitor 1 - front door (alternate, Janitor 2) Engineering Dept. chief - back door (alternate, Senior Engineer 1)	Signs should indicate that a shelter in place is in effect and that doors will not be opened until the "All Clear" is sounded.

Shelter Room Procedures:

<u>Procedure</u>	<u>Responsible Party</u>	<u>Needed Supplies/ Equipment/Rules</u>
Ascertain presence or whereabouts of all persons on employee/visitor sign-in sheets	Receptionist	Sign-in sheets
Seal windows and vents with plastic	Engineer 1, 2, and 3 (alternates, Sales manager, Accountant and Stock manager)	Shelter kit
Monitor radio broadcast for emergency messages	President (alternate, Vice President)	Shelter kit

All Clear Procedure:

<u>Procedure</u>	<u>Responsible Party</u>	<u>Needed Supplies/ Equipment/Rules</u>
“All Clear” message is received from emergency officials over television or radio	President (alternate, Vice President)	Radio from shelter kit
Employees will leave the shelter room and immediately go outside the building to pre-arranged meeting area	Individual employees	
Open all windows and doors (then leave bldg.)	Floor Monitors, Engineering Department Chief, other assigned employees	
Turn on ventilation systems (then leave bldg.)	Janitor 1 or 2	
Account for all employees and visitors	Receptionist	Employee and visitor sign- in sheets
Return to building when it has been thoroughly ventilated	To be determined by building engineers in advance of emergency	

SHELTER IN PLACE CHECKLIST
For Communication Employee (Receptionist)

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, the responsible employee (e.g., receptionist) shall:

- ☐ Announce “All employees and visitors – A shelter in place advisory has been issued. All employees and visitors should leave your current area and proceed to the first floor break room. Employees should make sure office windows and doors are closed before leaving.”
- ☐ Locate a cellular phone (from executive suite or sales office) and employee/visitor sign-in sheets and take them to the shelter in place room (break room).
- ☐ Determine from sign-in sheets whether all employees and visitors are accounted for. All employees and visitors should be in the shelter in place room within 3 minutes.
- ☐ When the “All Clear” is issued, take the sign-in sheets and leave the shelter room. Proceed to the pre-arranged meeting area outside the building.
- ☐ Account for employees and visitors using sign-in sheets. Report any discrepancies.
- ☐ When the building has been ventilated, return to the building and replace the cellular phone and sign-in sheets.

SHELTER IN PLACE CHECKLIST

For Maintenance Employees

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, the responsible employee (e.g., Chief of Maintenance) shall:

- ☐ Immediately proceed to the mechanicals room and turn off all air handling equipment (HVAC).
- ☐ Proceed to the break room for the remainder of the shelter in place. You should be in the break room within 3 minutes of the announcement.
- ☐ At the “All Clear,” leave the break room and proceed to the mechanicals room. Turn all ventilation equipment on.
- ☐ Leave the building and go to the pre-arranged meeting area outside. Check in with the receptionist.

SHELTER IN PLACE CHECKLIST

For Front Door Monitor

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, the responsible employee (e.g., janitor) shall:

- ☐ Collect the “Shelter In Place in Effect – NO ENTRY” sign and go to the front door of the office building.
- ☐ After 3 minutes have passed, place the sign on the outside of the door, lock it and proceed to the break room.
- ☐ Remain in the break room until the “All Clear” is announced.
- ☐ Unlock front door, take sign down, prop the door open, and go to the pre-arranged meeting area outside. Check in with the receptionist.
- ☐ Return to your station when the building has been completely ventilated and the you have been instructed to return to work. Upon returning to the building, close the front door and put the NO ENTRY sign back in its storage place.

SHELTER IN PLACE CHECKLIST

For Back Door Monitor

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, the responsible employee (e.g., engineering staff) shall:

- ☐ Collect the “Shelter In Place in Effect – NO ENTRY” sign and go to the back door of the office building.
- ☐ After 3 minutes have passed, place the sign on the outside of the door, lock it and proceed to the break room.
- ☐ Remain in the break room until the “All Clear” is announced.
- ☐ Unlock back door, take sign down, prop the door open, and go to the pre-arranged meeting area outside. Check in with the receptionist.
- ☐ After building is completely ventilated and upon instruction from the authorities, return to your office. Upon returning to the building, put the NO ENTRY sign back in its storage place and close the back door.

SHELTER IN PLACE CHECKLIST

For All Employees

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, each employee shall:

- ☐ Upon hearing the shelter in place announcement, make sure all office windows are closed and locked. Close your office door when you leave. Immediately go to the break room and escort any visitors to that room.
- ☐ Remain in the break room until the “All Clear” is announced. Immediately go outside to the pre-arranged meeting area and check in with the receptionist. Make sure any visitors are escorted to the meeting area as well.
- ☐ After the building is thoroughly ventilated and upon instruction from the authorities, return to your office.

SHELTER IN PLACE CHECKLIST

For Floor Monitors

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, the responsible employee shall:

- ☐ Make sure all employees and visitors on the floor have proceeded to the first floor break room.
- ☐ Check all offices and common areas to make sure windows are closed and locked. Close any open office doors. Make sure any fire doors are closed.
- ☐ Go to the break room for the duration of the shelter in place.
- ☐ When the “All Clear” is announced, return to your floor, open any operable windows and office doors, prop open fire doors.
- ☐ Go outside to the pre-arranged meeting area and check in with the receptionist.
- ☐ When the building is thoroughly ventilated and you are instructed to return to the building, close fire doors and windows in the common areas.

SHELTER IN PLACE CHECKLIST

For Window Sealing Crew

Responsible Employee _____ Checklist current as of: _____

Alternate Employee _____

When a shelter in place advisory is issued, the responsible employee (e.g., window sealing crew) shall:

- ☐ Close and lock office window and close door on the way to the break room.
- ☐ Remove plastic sheets and duct tape from shelter kit.
- ☐ Place plastic over window and seal edges with long strips of duct tape. Be sure tape securely overlaps all edges of the plastic.
- ☐ Place plastic overall vents and seal with long strips of duct tape. Be sure tape securely overlaps all edges of the plastic.
- ☐ When the “All Clear” is announced, immediately remove the plastic from the windows and vents. Open the windows, if operable.
- ☐ Go outside to the pre-arranged meeting area and check in with the receptionist.
- ☐ When the building is thoroughly ventilated and you are instructed to return, return to the break room, fold the plastic sheets and return to the shelter kit.

SHELTER IN PLACE CHECKLIST

For Door Sealing Crew

When a shelter in place advisory is issued, the responsible employee (e.g., door sealing crew) shall:

- ☐ Close and lock office window and close door on the way to the break room.
- ☐ Remove duct tape from shelter kit.
- ☐ Check with receptionist to assure that all employees have entered the break room (approximately 3 minutes after the announcement). Lock door to break room and seal edges with long strips of duct tape. Be sure tape securely overlaps all edges of the door.
- ☐ When the “All Clear” is announced, immediately remove the tape from the door.
- ☐ Go outside to the pre-arranged meeting area and check in with the receptionist.
- ☐ When the building is thoroughly ventilated and you are instructed to return, return to the break room. Also make sure that the battery-operated radio has been returned to the shelter kit.

Alert DC System

In the District, citizens and visitors can sign up for the **Alert DC System** which provides rapid text notification and update information during a major crisis or emergency. This system delivers important emergency alerts, notifications and updates on a range of devices including your:

- e-mail account [work, home, other]
- cell phone
- pager, BlackBerry
- wireless PDA



When an incident or emergency occurs, authorized DC Homeland Security & Emergency Management personnel can rapidly notify you using this community alert system. Alert DC is your personal connection to real-time updates, instructions on where to go, what to do, or what not to do, who to contact and other important information.

Alert DC is available to citizens of the District of Columbia as well as individuals traveling to or working in the District. Sign up for an account to receive alerts and emergency notifications today.

Note: Subscribers may be charged, as set forth in their wireless provider's contract, for messages delivered to their wireless devices.

- To register for an account, see **New User**.
- To manage or update an existing account, see **Log In**.
- For more information, visit www.hsema.dc.gov and click on “*Sign Up for Emergency Text Alerts*”

Emergency Go-Kits

A component of your emergency kit is your Go-Kit. Put the following (suggested) items together in a backpack or another easy to carry container in case you must evacuate quickly. Keep in mind additional items you may need based upon existing conditions or hazards. Prepare one Go-Kit for each family member and make sure each has an I.D. tag. You may not be at home when an emergency strikes so keep some additional supplies in your car and at work, considering any supplies you would need for your immediate safety.

Items for a 1 day “Go-Kit”	
<ul style="list-style-type: none"> • Identification, credit cards, cash • Water (1 gallon per person) • Non perishable food • Flashlight (battery or hand operated) • AM/FM radio (NOAA Weather Radio, if possible) • 12-hour lightstick • First aid kit and facial tissues 	<ul style="list-style-type: none"> • N95 particulate respirator mask • Emergency thermal blanket • Emergency poncho • Sanitary gloves • Emergency whistle • Family and emergency contact information • Prepaid Phone Card
Items for a 72 hour (3 day) “Go Kit”	
<ul style="list-style-type: none"> • Identification, credit cards, cash • 3 gallons of water (per person) • Non perishable food • Batteries • Flashlight (battery or hand operated) • AM/FM radio (NOAA Weather Radio, if possible) • 12-hour lightstick (3) • 30-piece first aid kit and facial tissues • N95 particulate respirator mask • Emergency thermal blanket • Emergency poncho • Sanitary gloves • Emergency Whistle 	<ul style="list-style-type: none"> • Multipurpose tool • Rain gear, sturdy shoes, a change of clothes • Sanitation and personal hygiene items • Cell phone with charger • Blankets, bedding, and/or sleeping bags. • Prescription medications and first aid supplies • Copies of personal documents (medication list and pertinent medical information, proof of address, deed/lease to home, passports, birth certificates, insurance policies) • Extra keys to your house and vehicle • Emergency preparedness manual • Prepaid Phone Card
Emergency Kit for Car	
<ul style="list-style-type: none"> • Case of bottled water • Non-perishable food • Manual can opener and basic eating utensils • Flashlight and extra batteries • Emergency whistle • Compass • Candles, matches, and a deep can to hold candles • Blankets • Extra clothes and shoes/boots • Road flares 	<ul style="list-style-type: none"> • Toilet paper and other personal care supplies • Multi-use tool (a Swiss Army knife is excellent for emergencies) • First aid kit • Small bills and coins • Small shovel • Jumper cables • Antifreeze/windshield washer fluid • List of emergency contact numbers • Prepaid phone card and/or car charger for mobile phone

ⁱ Individual with Limited English Proficiency – The term refers to an individual who does not speak English as his/her primary language and who has a limited ability to read, write, speak or understand English. Click the following link to access the FEMA multilingual webpage which provides flyers, brochures, tri-folds, press releases and public service announcements tailored to provide disaster preparedness, response, recovery and mitigation information for people with limited English proficiency levels. <http://www.fema.gov/media/resources/languages.shtm>

ⁱⁱ DHS Suspicious Package Response Checklist (Mar 2007)

ⁱⁱⁱ State of California Bomb Threat Telephone Calls (May 1997)

^{iv} National Institute for Chemical Studies (www.nicsinfo.org) *Shelter in Place at Your Office: A general guide for preparing a shelter in place plan in the workplace.*