Protective Measures Guide for U.S. Commercial Real Estate

September 2013

Homeland Security

Protective Measures Guide for U.S. Commercial Real Estate

September 2013

Disclaimer: The protective measures delineated in this guide are presented for guidance purposes only; they are not a requirement under any regulation or legislation. In addition, because of the wide variety in the types, sizes, and locations of commercial real estate, not all suggested protective measures will be relevant or applicable. This guide is not intended for nonmilitary Federal facilities in the U.S., whether government-owned, leased, or managed, or commercial office buildings with Federal or military tenants. The protective measures in this guide are based on practices that owners and operators of commercial real estate across the country have employed at their buildings. The ability to implement them at any specific facility will vary. This guide is not a complete source of information on protecting commercial office buildings. As such, owners, operators, and security personnel should leverage the full range of resources they have available to them and consider the specific nature of the threats when responding to changes in threat condition levels. Commercial real estate owners and operators should consider conducting a risk assessment at each individual property in order to decide which risks they consider applicable and what protective measures they intend to employ.

Prepared by:
Commercial Facilities Sector-Specific Agency,
Sector Outreach and Programs Division,
Office of Infrastructure Protection,
National Protection and Programs Directorate,
U.S. Department of Homeland Security

Table of Contents

This page intentionally left blank.

Introduction

Preventing terrorism, enhancing security, and ensuring resilience from disasters are core missions of the U.S. Department of Homeland Security (DHS). Accomplishing these missions necessitates building and fostering a collaborative environment in which the private sector and Federal, State, local, tribal, and territorial governments can better protect critical infrastructure. The Commercial Facilities (CF) Sector is one of 16 critical infrastructure sectors designated by DHS. Within the CF Sector, the Real Estate Subsector contains assets in which Americans live and work every day. The industry is designated as critical infrastructure because it is essential to the Nation's economic vitality and way of life. It is critical to the Department's vision of ensuring a homeland that is safe, secure, and resilient against terrorism and other natural and manmade hazards.

Within DHS, this overarching responsibility for critical infrastructure protection is delegated to the National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (IP), specifically the Sector Outreach & Programs Division[1] (SOPD) CF Section. Serving as the Sector-Specific Agency (SSA) for the CF Sector, the CF SSA works with its partners to address and highlight low-cost preparedness and risk management options in the products and tools it makes available to the private sector. For example, the CF SSA has produced a suite of protective measures guides that provides an overview of best practices and protective measures designed to assist owners and operators in planning and managing security at their facilities or events.[2]

This guide consists of contributions from the following partners:

- Beacon Capital Partners
- Building Owners and Managers Association International
- Jones Lang LaSalle
- Real Estate Roundtable
- Real Estate Information Sharing and Analysis Center
- Tishman Speyer
- Universal Protection Service

This *Protective Measures Guide for Commercial Real Estate* is designed to provide owners and operators of commercial office buildings with information that can be used to maintain a safe environment for occupants, employees, contractors, and visitors. The measures provide suggestions for successful planning, organizing, coordinating, communicating, operating, and training activities to augment the overall security posture at commercial office buildings. In addition, when contemplating appropriate protective measures to implement, owners and operators should consider their own knowledge of the property's operation and vulnerabilities, as well as the general surroundings and their location within the community and neighborhood. When implementing appropriate protective measures, owners and operators should make use of additional resources, from local law enforcement, first responders, and emergency management agencies. Some useful security resources have been listed in the appendices of this guide.

[1] For more information on IP and SOPD please visit http://www.dhs.gov/about-office-infrastructure-protection

[2] For more information on the CF SSA please visit http://www.dhs.gov/cfsector

This page intentionally left blank.

1. Commercial Real Estate Profile

1.1 Commercial Real Estate Overview

Americans live and work every day within Commercial Real Estate assets, which can range from one-story, single-unit office buildings to towering skyscrapers. The Commercial Real Estate industry comprises office buildings, large residential buildings, multi-family residential units, self storage facilities, and more. In addition, many large commercial office buildings contain other businesses, including restaurants, dry cleaners, drug stores, and daycare centers. According to the Real Estate Roundtable, "U.S. commercial real estate is worth approximately $5 trillion, including 4 billion sq. ft. of office space; 13 billion sq. ft. of industrial property; almost 9.5 billion sq. ft. of shopping center space; 4.4 million hotel rooms; and 33 million sq. ft. of rental apartment space." The industry also creates or supports approximately 9 million jobs.[3]

> "The Commercial Real Estate industry comprises office buildings, large residential buildings, multi-family residential units, self storage facilities, and more."

The buildings that comprise the Commercial Real Estate industry are mostly built in accordance with building codes that were never intended to prevent or minimize the impacts caused by manmade hazards such as terrorist attacks; however, the collapse or failure of these buildings can result in significant loss of life and

[3] http://www.rer.org/Media/Statistics_About_the_Real_Estate_Industry.aspx, (accessed June 28, 2013).

a severe effect on the economy. For the purposes of this guide, the protective measures will focus primarily on the subsets of Commercial Real Estate. Herein after, subsequent sections of this guide will refer to all Commercial Real Estate as "buildings" unless the topic refers to a specific subset.

1.1.1 High-Rise Buildings

High-rise buildings are an increasingly common sight where land is scarce, as in the centers of big cities, because of the high ratio of rentable floor space to area of land. A high-rise building is defined as a minimum architectural height of 35 meters (115 feet), and is automatically as a high-rise when it has a minimum of 12 floors whether or not the height is known.[4] Some of the largest high rise office buildings exceed 1 million square feet and are among the Nation's most prominent icons. Large residential or multi-family unit buildings are often high-rise buildings, which include apartments, condominiums, and cooperatives. The buildings typically contain only residential units; however, some mixed-use developments will have offices, hotel space, or apartments above street-level retail units.

1.1.2 Mixed-Use Buildings

A mixed-use building is defined as one that contains two or more functions, where each of the functions occupy a significant proportion of the building's total space.[5] Some mixed-use buildings will have offices, hotel space, or apartments above street-level retail units. More than two-thirds of all office buildings house administration and professional services. Banks and financial institutions make up 17% of office building use, with medical offices, government, and other entities account for the remainder.[6] A mixed-use building can feature two or more of the described uses, in any configuration.

1.1.3 Office Parks & Suburban Properties

Many corporations are now moving from urban high-rise buildings to suburban corporate campuses consisting of mostly low- and mid-rise buildings. As both technology and environmental policies evolve, physical location is becoming less critical for many workers. Office parks and business centers provide accessible, low-cost, flexible space, and green spaces that integrate pedestrian and vehicular movement.

[4] The Emporis Standards Committee, a leader in developing voluntary building standards and guidelines: http://www.emporis.com/building/standards/high-rise-building, (accessed June 28, 2013).

[5] The Council on Tall Buildings and Urban Habitat, an international not-for-profit organization supported by architecture, engineering, planning, development and construction professionals: http://www.ctbuh.org/TallBuildings/HeightStatistics/Criteria/tabid/446/language/en-US/Default.aspx, (accessed June 28, 2013).

[6] http://www.eia.gov/emeu/cbecs/pba99/office/office.html, (accessed June 28, 2013).

1.1.4 Medical Office Buildings

Medical office buildings are office and laboratory facilities constructed for the use of physicians and other health personnel and include, but are not limited to, ambulatory care centers and facilities used to provide diagnosis and treatment for medical, dental, or psychiatric outpatient care. Numerous arrivals and departures take place in such facilities, via many entrances and exits and may allow occupant traffic throughout the building.

1.1.5 Self Storage Facilities

The self storage industry has been one of the fastest-growing sectors of the United States commercial real estate industry over the period of the last 35 years according to the Self Storage Association. As of 2009, there were more than 46,500 primary self-storage facilities in the United States, with another 4,000 "secondary" facilities (The U.S. Census Bureau identifies "primary" such that self storage is the "primary" source of business revenue).[7] As of 2011, total self-storage rentable space in the U.S. was 2.3 billion square feet, a figure that represents more than 78 sq. miles of rentable self-storage space, under roof – or storage area more than three times the size of Manhattan Island (NY).

> "Many large commercial office buildings contain other businesses, including restaurants, dry cleaners, drug stores, and daycare centers."

1.1.6 Apartments, Condominiums, and Multi-Housing

The Nation's multifamily housing provides homes for over 23 million households.[8] These residential buildings generally feature controlled-access lobbies, common areas (e.g., meeting rooms and exercise rooms), on-site parking, and a staff to maintain the common areas and grounds of the building. Residential buildings can contain only residential units or may feature another function (e.g., retail) and may be classified as "Mixed-Use Buildings."

1.2 Key Vulnerabilities

Among the key vulnerabilities to Commercial Real Estate in the United States are the following:

- **Open public access:** While openness to the public is an important element for successful business operations and a feature common to most buildings; it contributes to their vulnerability. For security purposes, many buildings channel access through entry control points for screening. However, most buildings have no security to screen guests before they enter, or they have been constructed with an emphasis on ease of access and openness rather than security. Many

[7] http://www.selfstorage.org/ssa/Content/NavigationMenu/AboutSSA/FactSheet/default.htm, (accessed June 28, 2013).

[8] http://www.rer.org/Media/Statistics_About_the_Real_Estate_Industry.aspx, (accessed June 28, 2013).

buildings also have public spaces (e.g., retail) that are available during working and after hours. Building interiors can create opportunity for concealing items or act as staging areas for attacks. These factors can make security measures difficult to implement.

- **Building design:** Many buildings, particularly older ones, may not have been designed with security considerations in mind. Examples of such designs are those that do not include perimeter buffer zones, stand-off barriers, or explosive countermeasures. Other examples include large areas of glass that are not shatter or blast resistant, structural supports that cannot handle large overpressures from explosives, and doors and windows that are not tamper-resistant. The actual design, location, and building height may also contribute to its overall vulnerability to adverse health effects, injury, or progressive collapse.

- **Multiple locations to place explosives or hazardous agents:** Buildings have numerous locations where an explosives package (e.g., a backpack) or a container with hazardous agents can be left without being immediately noticed. These include public areas (both inside and outside), building occupant areas, public bathrooms, trash containers, mailboxes, planters, counters, and decorative fixtures.
- **Multi-use facilities:** Buildings may be integrated with other facilities or infrastructures, such as mass transit, hotels, convention centers, universities, and airports. Each of these situations has its own site- and situation-specific vulnerabilities.
- **Tenant risk profile:** Some buildings house high-risk tenants and special-use tenants (e.g., government, banking) or a mixture of both high- and low-risk tenants.
- **Access by suppliers, vendors, and maintenance workers to nonpublic areas:** Many people other than building employees are given access to areas of the facility that are not open to the public. Such individuals include construction crews, maintenance personnel, messengers, and cleaning crews. These individuals may not be screened in some buildings, and their vehicles often enter through loading docks, mailrooms, or service entrances that may not be secured or monitored.
- **Vehicular control:** In most instances, owners of commercial office buildings have no control over the right-of-way associated with the sidewalk and street access surrounding their buildings. Many buildings do not allow for buffer zones between the building and unscreened vehicles. Unregulated traffic and pedestrian movement increases security concerns around the perimeter or within the perimeter of the building.

> “Many buildings, particularly older ones, may not have been designed with security considerations in mind.”

- **Parking control:** Buildings can be vulnerable within their own parking lots or parking garages where tenants and visitors have access with little or no screening.

- **Unprotected building management systems:**
  - **Heating, ventilating, and air conditioning (HVAC) systems:** In some buildings, access to HVAC systems is not controlled or monitored. Air intakes may be in publicly accessible areas, and HVAC equipment may not be in secured rooms equipped with intrusion-detection equipment. In some cases, it may be necessary to shut down these systems to prevent outdoor-borne contaminants from entering a building, such as smoke from a nearby fire or contaminated area from a HAZMAT spill. Likewise, unprotected HVAC systems could be vulnerable to the release and introduction of a biological or chemical agent which could quickly contaminate a building. Unprotected and/or unknown access points to HVAC dependent computerized building management systems also present a significant vulnerability. HVAC components with networking capability are especially vulnerable if they are connected to the public Internet, either intentionally or as part of a system to allow technicians to connect remotely.

> "Many people other than building employees are given access to areas of the facility that are not open to the public."

  - **Utility Services:** Some buildings have not secured and do not monitor the utility services (including electric power, natural gas, telecommunications, emergency generator, and water supply) for intrusion. Computer systems that regulate and monitor the provision of utility services can also be vulnerable to unauthorized access and manipulation.
  - **Access Control:** Buildings rely upon access control systems, such as badge readers, smart cards, and electronic turnstiles to manage the flow of authorized persons into buildings and sensitive areas. A weakness in an underlying computer system could result in unauthorized physical access to facilities and assets.
- **Mailroom and messenger operations:** All buildings provide for the delivery of daily and periodic mail by the U.S. Postal Service, commercial overnight mail services, and messenger groups. Some facilities are contained within tenant spaces while others are in common areas controlled by the building ownership. Suspicious packages and envelopes can and do pose a threat to the daily operation of a building.
- **Proximity to other properties:** Adjacent properties may also provide opportunities of convenience to adversaries if they do not have the same level of access control on their vehicle movements, parking, building access, and roof access. Similarly, potential site access through utility tunnels, corridors, and manholes creates access vulnerability.
- **Limited employee background checks:** Many building tenants conduct minimal or no background checks when hiring staff.
- **Limited security staff:** Many building owners or operators have only a small security staff and rely mostly on local law enforcement to handle incidents. Larger buildings may have a larger

security staff, sometimes under a contract arrangement with a private security firm. The extent to which these personnel are trained and equipped to deal with natural or man-made incidents varies widely from State to State and city jurisdictions.

- **Lack of exercises for emergency plans:** While some buildings have documented emergency operations plans, exercises of the plans are limited. It is difficult to interrupt normal business activities to conduct an emergency exercise. Coordination of building emergency plans with local emergency responders may be lacking.

2. Terrorist Objectives

> “New evidence suggests that future attacks may occur more frequently and involve fewer people in the planning and implementation process.”

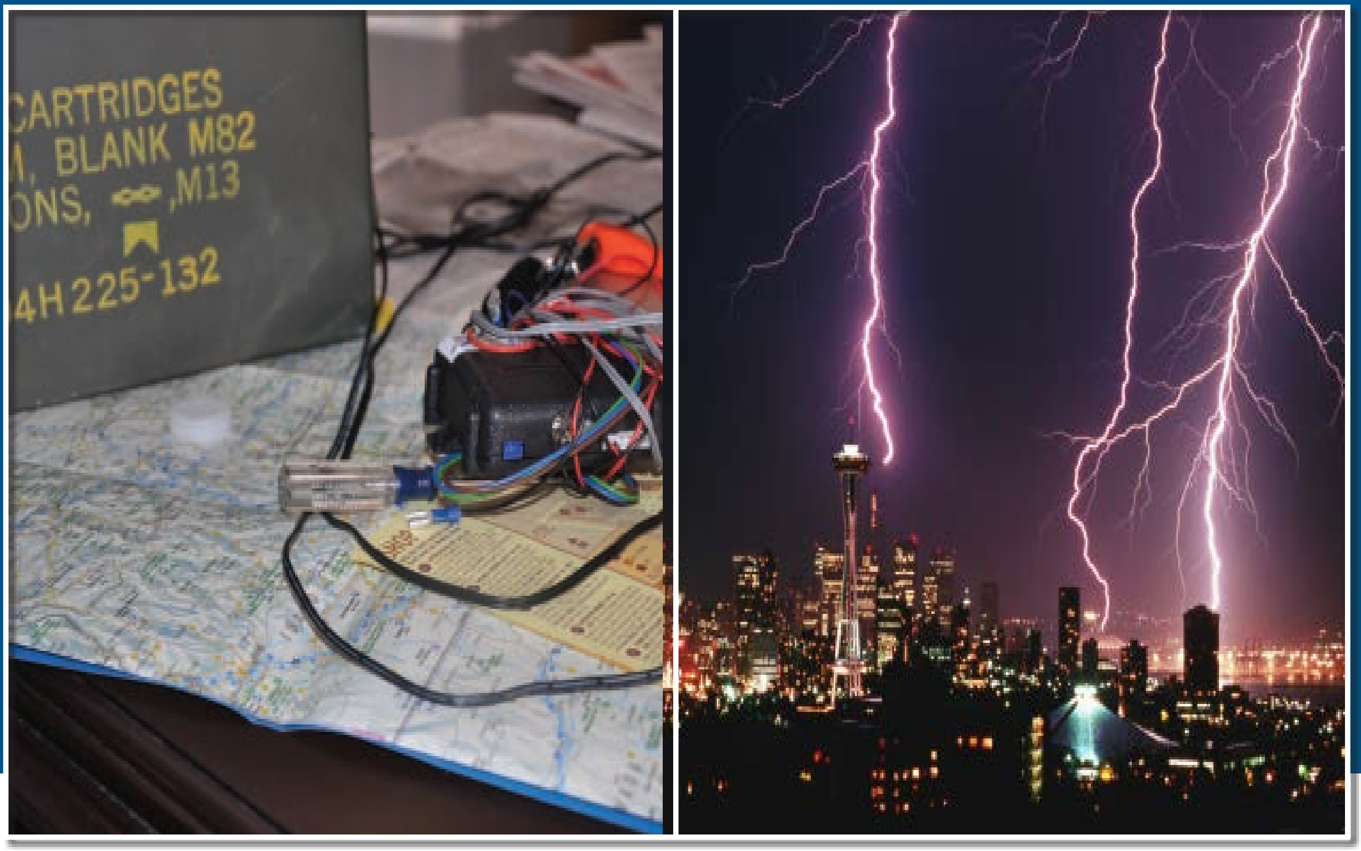
Terrorists have demonstrated an understanding of the potential consequences of carefully planned attacks within the United States. Whether the terrorists belong to a transnational organization such as al Qaeda, operate as lone offenders, or homegrown violent extremists, their motivations include, but are not limited to, advancing ideological and political agendas that address religious and policy grievances. Generally, to achieve these ends, terrorists seek to destroy, incapacitate, or exploit critical infrastructure across the United States in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence in government leadership. New evidence suggests that future attacks may occur more frequently and involve fewer people in the planning and implementation processes.

Inflicting mass casualties in the form of fatalities, injuries, and illness is one of the major objectives of many terrorist acts, and these consequences may occur both at the targeted facility and in the surrounding area. Those who would seek to damage or destroy a facility may do so with the intention of shutting down or degrading facility operations or releasing hazardous materials to the surrounding area. Disruption of the targeted site without inflicting actual damage can interfere with building operations and public access, and tampering with building products can render them dangerous or unusable.

Theft of equipment, materials, or products can be intended to divert these resources to other uses or to reap financial gain from their resale. Theft of information can be intended to acquire insight that is not publicly available, gaining data that can be used in carrying out attacks.

Deteriorating public morale and confidence in a facility's security following an incident produces an ongoing psychological impact that causes economic losses and reputational harm - an objective for many terrorists. It is important for owners and operators to understand terrorist motivations and objectives that may lead to attacks against the Nation's critical infrastructure, so they may take appropriate protective measures to reduce risk and increase resilience at their facilities.

3. Threats and Hazards



> “Terrorists, violent criminals, and transnational organizations have a variety of weapons and tactics to achieve their objectives.”

The best way to manage risk is to understand a building’s potential vulnerability to threats and hazards and to train building services personnel, including security, parking, janitorial, and landscaping, to recognize and report potentially significant incidents. The purpose of this section is to provide building managers examples and scenarios that may affect their specific property.

For the purposes of this guide, manmade hazards are potential acts of terrorism to include any threat, activity, or attack with the element of human intent. Manmade hazards are typically associated with a criminal or terrorist attack using a weapon such as an explosive, biological, or chemical agent. Manmade hazards are distinct from hazards involving human error or negligence, which are defined as “accidents” (Section 3.2).

3.1 Manmade Hazards

Terrorists, violent extremists, lone offenders, as well as violent criminals and mentally unstable individuals may pose a risk to a building. The attack methods listed in this section are the manner and means an adversary may use to cause harm to a target. Terrorists, violent criminals, and transnational organizations have a variety of weapons and tactics available to achieve their objectives, and they have demonstrated an ability to plan and conduct complex, simultaneous attacks against multiple targets. Individuals, a small team, or larger groups acting in a coordinated fashion can carry out an attack. Possible manmade hazards are outlined below.

3.1.1 Improvised Explosive Devices

> “In 2009, the FBI disrupted a plot to detonate IEDs, with ingredients that could be acquired from beauty supply stores, on the New York City subway system.”

An improvised explosive device (IED), or homemade bomb, can be constructed of commonly available materials; construction explosives such as dynamite, stolen commercial or military-grade explosives; or homemade explosives. An IED can be carried into a venue by an individual, such as a suicide bomber or can be deposited in an unnoticed location for detonation by timer or by remote control.

IEDs have been used extensively overseas and are also popularized in part by such Jihadist publications as *Inspire* magazine and the *Lone Mujahid Pocketbook*, which detail how to make IEDs with common household products. Two recent examples illustrate the means which IEDs can be constructed from common materials and hidden in plain sight:

- In 2010, two packages, each containing an IED concealed within laser printers, were discovered aboard cargo planes bound for the United States. Both packages were addressed to outdated addresses of Jewish facilities in the Chicago area; however, the packages were discovered in England and Dubai, and it is believed the planes and not the facilities were the actual targets.
- In 2009, the FBI disrupted a plot to detonate IEDs on the New York City subway system with ingredients that could be acquired from beauty supply stores.

3.1.2 Vehicle-Borne Improvised Explosive Devices

Vehicle-borne IEDs (VBIEDs) are improvised explosive devices that are loaded into a car or truck, on a motorcycle, or bicycle. The vehicle can be parked close to the targeted venue, placed where large numbers of people gather adjacent to the venue perimeter, or driven through barriers and then detonated. VBIEDs are much larger and more dangerous than IEDs because they allow for a higher quantity of explosives to be delivered. Surveillance by terrorist(s) often precedes IED and VBIED attacks. Overseas, VBIED attacks have been used in concert with other tactics, such as small arms (e.g., breaching a fortified location with a VBIED then employing small arms) and IEDs (e.g., detonating secondary explosions after a VBIED attack draws first responders).

VBIEDs are a common means of attack throughout the world. A VBIED was deployed against the Alfred P. Murrah Federal Building in Oklahoma City in April 1995. The Oklahoma blast claimed 168 lives, including 19 children, and injured more than 680 people. The blast destroyed or damaged 324 buildings within a sixteen-block radius, destroyed or burned 86 cars, and shattered glass in 258 nearby buildings. The bomb was estimated to have caused at least $652 million worth of damage. Another VBIED example is the February 1993 car bombing of the World Trade Center (WTC). On February 26, 1993, a charge of 1,200 to 1,500 pounds of homemade explosive was detonated in an Econoline van on the B-2 level of the parking garage of the WTC in New York City. The blast produced a crater roughly 150 feet in diameter and five floors deep. Six people were killed, and 1,042 were wounded. Damage was estimated at $500 million.[9] Two more recent examples of attempts to use VBIEDs include a May 2010 attempt to detonate a crudely made gasoline and propane bomb in a Nissan Pathfinder on a busy Saturday night in Times Square, and the November 2010 arrest of a man in Portland, Oregon after an attempt to detonate what he believed to be an explosives-laden van at a tree lighting ceremony.

> “Overseas, VBIED attacks have been used in concert with other tactics, such as small arms and IEDs.”

3.1.3 Arson and Improvised Incendiary Devices

Intentional fires can be set by using highly flammable materials such as gasoline. Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson could also be used in conjunction with other forms of attack such as a small arms assault, or can be a second order effect of another form of attack such as an IED. Arson is a common threat both during and after normal business hours. *Inspire*, al Qaeda’s English language online magazine, has suggested arson as a tactic. Its ninth issue includes detailed instructions and illustrations on assembling and using an improvised incendiary device (IID) referred to as an “ember bomb” to cause wildfires, as well as information on several ignition and timing mechanisms.

3.1.4 Small Arms Attack (Including Active Shooter)

Small arms, including automatic rifles, grenade launchers, shoulder-fired missiles, or other such weaponry, can be used to target people (e.g., shooting of civilians) or venues (e.g., standoff assault from outside a perimeter fence). An active shooter is an armed individual who uses deadly force on other persons and continues to do so while having unrestricted access to additional victims in a confined and populated area. Active shooters usually use firearms and select their victims at random. Active shooter situations are unpredictable and evolve quickly. This tactic was employed by the gunman of the July 2012 mass shooting at an Aurora, Colorado movie theater that killed 12 and injured 58 others.

[9] FEMA (Federal Emergency Management Agency), 1993, *The World Trade Center Bombing: Report and Analysis*, provided by *Fire Engineering* for FEMA, U.S. Fire Administration, National Fire Data Center.

3.1.5 Chemical Attack

Terrorists have exploited toxic chemicals as a weapon. Industrial chemicals transported or brought near an outdoor venue or large gathering of people can be dispersed by explosives, sprayers, or other dissemination devices. Chemical warfare agents such as sarin and VX also can be used as potential weapons. Although not readily available, historically these chemical warfare agents have been produced and used by terrorists. The most notable instance of terrorist use of chemical weapons is the 1995 sarin attack on the Tokyo subway, which killed 12 people and affected thousands more.

3.1.6 Biological Attack

Biological pathogens such as anthrax and plague can cause disease and are used by terrorists because of the pathogens' ability to cause mass casualties and exhaust emergency response resources. Biological agents can be dispersed in the atmosphere via crop-dusting aircraft or other airborne medium; introduced into an area or directly into a building at an outdoor venue through its heating, ventilation, and air conditioning (HVAC) system; used to contaminate food or drink; or spread by contact (e.g., via contaminated letters delivered by mail). A biological attack may involve colorless or odorless agents, and symptoms of exposure may be undetected for days or weeks afterwards. In 1984, members of a religious cult contaminated the salad bars of 10 restaurants in The Dalles, Oregon to influence a local election, resulting in 751 confirmed cases of salmonellosis. In 2001, letters containing anthrax spores were mailed to several news media offices and two U.S. Senators, killing five people and infecting 17 others. More recently, the Fall 2010 issue of *Inspire* magazine called on readers to "develop an effective poison with the proper method of delivery," citing cyanide, ricin, and botulinum toxin as examples of poisons that could be used. In June 2011, authorities in Indonesia arrested violent extremists plotting to use cyanide to poison police food.

> "A biological attack may involve colorless or odorless agents, and symptoms of exposure may be undetected for days."

3.1.7 Radiological Attack

Although weapons-grade nuclear material is relatively difficult to obtain, some sources of radiological material are more readily available and easier to deliver. Radiological materials include radioactive material from a variety of sources, such as medical or industrial equipment. In radiological dispersion devices, often called "dirty bombs," terrorists can attach radiological material to an explosive to create a wide area of contamination. Terrorists can also introduce radiological material or contaminated materials into a building directly or through its HVAC system. An example of a radiological attack was the 2006 death of Alexander Valterovich Litvinenko, a former Soviet KGB officer poisoned by Polonium-210, a radioactive material that had been slipped into his tea.[10]

[10] http://www.guardian.co.uk/world/2011/oct/18/alexander-litvinenko-killers-big-mistake, (accessed June 28, 2013).

3.1.8 Aircraft Attack

Terrorists can and have previously demonstrated the ability to leverage aircraft of any size to deliver attackers, explosives, or hazardous materials to a target. The aircraft itself can also be used as a weapon. The most notable examples are the September 11, 2001 attacks on the Pentagon and the World Trade Center in New York City. Another example occurred in February 2010 when a lone offender deliberately crashed his small plane into a seven-story building in Austin, Texas that housed an Internal Revenue Service field office.

3.1.9 Maritime Attack

Ships and boats of various sizes can be used transport arms and explosives and gain access. The vessel itself also can be used as a weapon. Prior to the 2008 attacks in Mumbai, terrorists used a fishing vessel and small boats to transport arms and explosives and gain access to the city. On October 12, 2000, a small craft laden with explosives rammed the USS *Cole* while it was refueling in the Yemeni port of Aden. The attack killed 17 American sailors and injured several more.

3.1.10 Cyber Attack

Malicious actors, such as criminals, insiders, politically motivated hacktivists, and terrorists can infiltrate data processing, transfer, storage, communications, and security and surveillance systems to cause economic and operational damage or exploit proprietary information. Attackers can alter, steal, or render information unusable. Information systems can be attacked with the intent of overloading the equipment (e.g., denial-of-service attacks). Attacks on control systems may also result in disruption of or misinformation about facilities, mechanical systems such as elevators, and emergency communications, that could potentially endanger occupants. Recent examples of cyber attacks affecting the Real Estate Subsector include malicious insiders adjusting computerized HVAC systems,[11] unauthorized actors breaching Internet remote access systems to adjust temperature settings in the building's Energy Management System,[12] and security researchers demonstrating the potential for unauthorized facility admittance by tricking smart card access control systems.[13]

3.1.11 Sabotage (Including Insider Threat)

The disruption, damage, or destruction of a property through sabotage, and the introduction of hazardous materials into a building are of concern. Sabotage can be perpetrated by employees or by outsiders, such as contractors. Employees may pose a greater threat because they have special knowledge of and access to the venue. A disgruntled employee can easily undermine even the best security plan. An example of an insider threat was Al Qaeda operative Dhiren Barot being tasked by one of his terrorist cell members

[11] http://www.darkreading.com/insider-threat/167801100/security/privacy/218300006/security-guard-busted-for-hacking-hospital-s-hvac-patient-information-computers.html, (accessed June 28, 2013).

[12] http://www.darkreading.com/insider-threat/167801100/security/privacy/218300006/security-guard-busted-for-hacking-hospital-s-hvac-patient-information-computers.html, (accessed June 28, 2013).

[13] http://www.securitydirectornews.com/commercial-and-enterprise/researchers-hack-popular-smartcard-used-access-control, (accessed June 28, 2013).

to work at a hotel to learn how to disable fire and security alarms.

A vulnerability of the Commercial Real Estate industry is the lack of security controls with regard to cleaning and groundskeeping services, including the issue of illegal subcontracting. Many janitors, for example, have nearly unlimited access to a building's sensitive areas during and after working hours. At issue are those cleaning services who either fail to conduct significant background checks or participate in unscrupulous activities designed to defraud the United States, harbor illegal aliens for profit, or evade payment of Federal employment taxes. The lack of these types of security controls can allow terrorists, criminals, and former or disgruntled employees to infiltrate and exploit a building.

3.1.12 Assassination, Kidnapping, and Hostage-Taking

Many terrorist acts have involved tactics such as kidnapping, hostage-taking, and assassination of key personnel. Recent examples include:

- In June 2012, a mentally-unbalanced gunman claiming links to al Qaeda was arrested after taking hostages in a bank in Toulouse, France. French authorities arrested the man, and the hostages were released unharmed.[14]
- In June 2011, following the death of Osama Bin Laden, a Web site associated with al Qaeda called upon sympathizers to target and kill several prominent Americans at their homes which included corporate executives, business leaders, and defense contractors.
- In November 2010, Roshonara Choudhry, a radicalized Briton, attempted to assassinate former British government Minister Stephen Timms at the Beckton Globe, a community center in East London. Choudhry was inspired to stab Timms with a small knife for his support of the Iraq War after watching online sermons from Anwar al-Awlaki, the extremist preacher and suspected mastermind of the recent airline "ink cartridge bomb" plot (see Section 3.1.1 Improvised Explosive Devices).[15]
- In September 2010, a mentally-unbalanced gunman with explosives took three people hostage in the lobby of the Discovery Communications Headquarters building in Silver Spring, MD before he was shot and killed by police.

3.1.13 Civil Unrest/Disruption

Protests and demonstrations, even if directed at another's property, can disrupt a building's operations or lead to violence. Public spaces near your building, which are properties open to the public 24 hours a day, could become locations for individuals to set up campsites. The most recent example of civil unrest was the Occupy Wall Street (OWS) movement, which began in New York City's Zucotti Park in 2011 and spread protests and encampments

[14] http://www.guardian.co.uk/world/2012/jun/20/toulouse-bank-hostages-freed-police-raid, (accessed June 28, 2013).

[15] http://www.guardian.co.uk/uk/2010/nov/02/stephen-timms-attacker-guilty, (accessed June 28, 2013).

throughout the United States. Though the OWS protesters remained largely peaceful in 2011, there were instances of some protests becoming violent both domestically (including Oakland, CA and Seattle, WA) and internationally (including London and Rome). Encampments can become a haven for criminal and drug activity, and cause disruptions to nearby buildings. For some protests, key calendar social recognition dates should be considered by owners and operators to prepare in advance for potential disruptions.

3.2 Accidents

Buildings must also prepare for accidents on their premises or in their immediate vicinity, such as chemical spills and electrical fires. Industrial accidents (e.g., train derailments), structural collapses, or power outages beyond venue perimeters also could affect buildings. These are some recent examples that illustrate the unpredictability and the cascading effects of accidents:

- In May 2012, a 115,000 volt transformer exploded in a Boston substation, resulting in a fire and a blackout in the Back Bay and East End areas of the city. It was initially feared the smoke from the fire was toxic but was determined to be from mineral oil which is used to cool the transformer.[16] The blackout left thousands of frustrated residents and businesses without power for days, resulting in significant business disruptions and losses.
- In July 2007, a 24-inch, underground steam pipe built in 1924 exploded in New York City during evening rush hour. The explosion killed one and hurt twenty; sent steam, water, and debris into the air; and created a crater on Lexington Avenue near Grand Central Station that swallowed a truck.[17]
- In December 2004, faulty wiring caused a fire to sweep through floors 29 and 30 of 135 South La Salle Street, a prominent commercial office building in Chicago, IL. There were no fatalities as a result of the fire; however, several occupants were treated for smoke inhalation. At the time of the fire, sprinklers were being installed as a result of the Cook County Administration Building fire.[18]
- In October 2003, a fire began in a supply room at the Cook County Administration Building in Chicago, IL and resulted in six deaths and several injuries because of smoke inhalation. Two factors contributed to the tragedy: 1) flames spread throughout the supply room and its larger suite, and smoke spread throughout the 12th floor and into the southeast stairway where the victims were trapped; and 2) the 37-story building did not have sprinklers above the lobby as it was built before codes required sprinklers on every floor in skyscrapers.[19] The incident sparked outrage and resulted in a city-wide review of fire policy.

[16] http://boston.cbslocal.com/2012/03/13/firefighters-battle-4-alarm-blaze-near-back-bay-hilton/, (accessed June 28, 2013).

[17] http://cityroom.blogs.nytimes.com/2007/07/18/buildings-evacuated-after-midtown-explosion/, (accessed June 28, 2013).

[18] http://www.chicagotribune.com/news/local/chi-0412220352dec22,0,144514.story, (accessed June 28, 2013).

[19] http://www.fire.nist.gov/bfrlpubs/NIST_SP-1021.pdf, (accessed June 28, 2013).

3.3 Natural Hazards

A natural hazard such as a hurricane, tornado, earthquake, flood, or severe storm may occur without warning and severely impact operations at a building. Though the majority of this guide will focus on reducing the risk of manmade hazards, buildings should also plan for all hazards, including natural disasters and extreme weather.

3.4 Pandemics and Public Health Emergencies

Public health emergencies affect communities and their citizens and, depending on their severity, can severely disrupt the economy and society. For example, an epidemic occurs when an infectious disease spreads rapidly to many people.[20] According to the World Health Organization, the 2003 Severe Acute Respiratory Syndrome (SARS) epidemic took the lives of nearly 774 people worldwide.[21] More recently, the Centers for Disease Control (CDC) reported a West Nile virus outbreak in 2012 as the largest ever seen in the United States.[22]

A pandemic is a global disease outbreak. A flu pandemic can occur when a new influenza A virus emerges, such as H1N1, against which no one is immune. There have been four pandemics since 1918, the latest emerging in 2009 with the first diagnosis of H1N1. In June 2009, the World Health Organization announced that the H1N1 virus had met the definitional threshold of a pandemic. The CDC estimates 43 million to 89 million people had H1N1 between April 2009 and April 2010, resulting in an estimated 8,870 to 18,300 H1N1 related deaths.

Whether an outbreak is circumscribed to a particular community or across a large region as in a pandemic, public health emergencies and their associated impacts – absenteeism, event cancellations, travel bans, business and school closures – can cause severe disruptions to a building's operations.

[20] http://www.webmd.com/cold-and-flu/what-are-epidemics-pandemics-outbreaks, (accessed June 28, 2013).

[21] http://www.who.int/csr/sars/country/table2004_04_21/en/index.html, (accessed June 28, 2013).

[22] http://www.cnn.com/2012/08/22/health/west-nile-virus/index.html?hpt=hp_t1, (accessed June 28, 2013).

4. Protective Measures

Protective measures include equipment, personnel, training, and procedures designed to protect an event or facility against threats and mitigate the effects of an attack. Protective measures are designed to meet one or more of the following objectives:

Devalue Lower the appeal of a facility to malicious actors; that is, make the facility less interesting as a target.

Detect Spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.

Deter Make the facility more difficult to attack successfully.

Defend Respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack.

Some protective measures are designed to be implemented on a permanent basis to serve as routine protection for a facility. Such measures are sometimes referred to as baseline countermeasures. Others are implemented or are increased in their application only during times of heightened alert.

The implementation of protective measures involves the commitment of resources in the form of people, equipment, materials, time, and money. Building owners and operators need to coordinate and cooperate with local law enforcement, emergency responders, and Federal, State, local, tribal, and territorial government agencies with regard to what measures to implement; how extensive they should be; and how long they should be carried out in order to maximize security while staying within the bounds of available resources.

To assist in the decisionmaking process, a risk-based protective posture is recommended. DHS recognizes three factors involved in calculating risk:

- **Threat:** A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. The probability of a manmade threat is determined by examining the intent of an adversary versus the capability of an adversary.
- **Vulnerability:** Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- **Consequence:** Effect of an event, incident, or occurrence. The consequence is determined by multiple factors that include, but are not limited to, the loss of life, physical damage to a facility, the economic impact, and the psychosocial impact of an event.

Each building should conduct its own risk assessment and tailor its plans according to the risk at its facility. Risk assessments are discussed in greater detail in section 4.1. Owners and operators are also encouraged to have a scalable approach to managing risk. The capability to increase protective measures based upon the threats to a building at any given time, and ensuring each increase in the protective posture includes applying every action recommended in the lower risk postures as well, should be considered in the development of this scalable approach.

> “Each building should conduct its own risk assessment and tailor its plans to the risk at its facility.”

The Department of Homeland Security utilizes the National Terrorism Advisory System[23], or NTAS, to communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. NTAS Alerts will only be issued when credible information is available. These alerts will include a clear statement that there is an elevated threat or imminent threat.

Elevated Threat	Warns of a credible terrorist threat against the United States.
Imminent Threat	Warns of a credible, specific, and impending terrorist threat against the United States.

Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat.

[23] To register for NTAS alerts, please visit *http://www.dhs.gov/files/programs/ntas.shtm*

NTAS Alerts contain a sunset provision indicating a specific date when the alert expires—there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

The protective measures described in this chapter are designed to provide information and assistance to building managers in making decisions on managing risk. When implementing protective measures, owners and operators should make use of additional resources from local law enforcement and emergency management agencies, in addition to the security resources listed in the appendices. The protective measures described in this chapter are grouped into the following categories:

- Planning and Preparedness
- Incident Management
- Personnel
- Physical Security Systems
- Credentialing
- Signage and Notification
- Barriers
- Communication, Networking, and Notification
- Monitoring, Surveillance, and Inspection
- Information Security and Cybersecurity
- Infrastructure Interdependencies

> “When implementing protective measures, owners and operators should make use of additional resources from local law enforcement and emergency management agencies.”

Measures for use during an elevated or imminent threat to your facility, geographic area, or industry are given at the end of each section.

4.1 Planning and Preparedness

Buildings should conduct threat, vulnerability, and risk assessments to determine a property’s relative levels of risk and to help identify the best and most cost-effective mitigation measures for their own, unique security needs. *BIPS 06/FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks against Buildings, 2nd Edition*, discusses the assessment process, asset value assessment, threat/hazard assessment, vulnerability assessment, risk assessment, and risk management. The publication also provides a Building Vulnerability Assessment Checklist. BIPS 06/FEMA 426 is a particularly helpful reference manual for new buildings during the design process, as well as for existing buildings going through a renovation.

Security audits should be conducted on a periodic basis, and after any changes in your security profile - such as a change in occupancy, change in operation, or time of year. Include assessments of other critical activities and operations in the vicinity for example, airports, chemical plants, government buildings, pipelines, rail lines, transportation/subway terminals, and public assembly venues, to determine if there is any potential for them to cause increased security risks to the building. Based on these analyses, develop a comprehensive security plan, emergency response plan (to include evacuation and shelter-in-place), and business continuity plan for the building. See section 6: Key Federal Protective Programs, for the U.S. Department of Homeland Security *Business Continuity Planning Suite* (BCP), which consists of three main components: BCP training, automated BCP and disaster recovery plan generators, and a self-directed exercise for testing an implemented BCP. Also, Ready Business assists businesses in developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards, which can be found at *http://www.ready.gov/business*.

Buildings should also consult corporate level and local jurisdictional plans, where applicable, to ensure the individual property's procedures do not conflict with corporate guidance, local code, or State and local emergency response agencies. Buildings should then develop their own property level plans that complement corporate and local level plans, but should also provide more detailed information addressing their property's specific needs. Plans must be developed and tested prior to an emergency to ensure preparedness.

Roles and Responsibilities

- Designate an experienced, supervisory-level employee of the building manager's organization to lead all security-related activities in the building.
- Form an interdisciplinary stakeholder group, comprised of the building's various departmental/contracted managers, to consult with the chief security officer.
- Involve the interdisciplinary stakeholder group, local law enforcement, and local emergency management in all levels of security planning.
- Develop a notification protocol that outlines who should be contacted in emergencies (when the building is open to the public and during off-hours). Designate who is to contact whom both internal and external to the building and the order in which they should be notified. Ensure the notification list is current.

- Ensure one or more building management employees who are familiar with the building's security, emergency response, and business continuity plans are available for deployment at all times.
- Establish a liaison and maintain regular communication with DHS, FBI, State Homeland Security Advisors, public health organizations, and industry organizations to enhance information exchange, track threat conditions, and support investigations. For example, the DHS Protective Security Advisor (PSA) Program provides DHS security experts in communities around the country as the link between State, local, tribal, and territorial organizations and DHS infrastructure protection resources. See section 6: Key Federal Protective Programs for more on the PSA Program.

- Identify outside vendor organizations that are vital to response and recovery operations. Encourage these key crisis vendors to develop and share their business continuity plans with regard to their own firm and their response to your building.
- Conduct regular drills and tabletop exercises with building management, tenant organizations, and neighbors. Involve local emergency responders in drills and exercises.
- Clarify agency emergency response and security responsibilities between building management and relevant Federal, State, and local emergency response agencies.
- Designate employees who will have responsibility for media interactions and dealing with the public in the event of an incident. These employees may be remote to the site; however, they should be aware of all plans, protocols, and included in training exercises. Develop policies and procedures for such interactions, and develop templates for messaging prior to incidents. Care should also be taken to understand any outside legal authorities that might be needed.
- Involve all employees at several levels in emergency response and security planning. Include building tenants, parking, and security personnel, as well as all key crisis vendors, and consider third-party evaluation and verification of plans.

Assessments

- Work with local law enforcement or a third party vendor to conduct a threat analysis, vulnerability assessment, consequence analysis, risk assessment, and security audit of the venue. Ensure that all information obtained by these efforts is kept confidential and that access is restricted.
- Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis. Include assessments of other activities and operations in the vicinity (e.g., airports, chemical plants, government buildings, pipelines, rail lines, transportation/subway terminals, public assembly venues) to determine if there is any potential for them to increase security risks to the building.
- Consider the following to determine the most likely threats to your building:
  - History of a threat type to the facility, the area, and the industry.
  - Visibility or symbolic importance of the building.
  - Crime trends and local gang activity.
  - Other adversarial groups and their capabilities.
  - High-profile or controversial tenants, occupants, visitors, or special events (e.g., may be televised) at the facility.
  - Natural hazard trends that would cause the building to be evacuated or for occupants to shelter in place. Evaluate the probable amount of warning time for each hazard. There may be 24 hours or more notice for a hurricane; however, there may be minimal or no warming for lightning or a tornado.

- Consider the following to identify vulnerabilities and areas of weakness that could result in serious consequences:
  - Physical features or operational attributes that may leave the building open to exploitation to a given hazard. Vulnerabilities may be associated with physical, cyber, or human elements (e.g., areas where large crowds congregate, limited access controls, open areas with limited security controls, and difficulty hearing emergency or evacuation announcements).
  - Appropriate level of vulnerability assessment or strategy (e.g., self-assessment, third-party assessment, expert reviews, or Federal/State-led assessment) and methodology.
  - Benefits of existing protective programs.
  - The impact your facility has on the surrounding area. For example, street closures associated with a special event or crowds associated with an evacuation may impact businesses and homeowners in the vicinity. Meet with neighboring businesses to discuss potential problems and to obtain input from the surrounding community.
  - Location of evacuation points identified and used by groups within the building and surrounding neighborhood.
- Consider the Integrated Rapid Visual Screening (IRVS)/BIPS 04 to conduct a simple and quick assessment. The IRVS facilitates obtaining scores for a risk assessment rating based on visual inspection. The IRVS manual of instructions and software can be found at http://www.dhs.gov/bips-04-integrated-rapid-visual-screening-series-irvs-buildings. In addition, *FEMA 452: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings* outlines methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. The methods presented provide a means to assess risks and to make decisions about how to mitigate them. This how-to guide can be found at http://www.fema.gov/library/viewRecord.do?id=1938.

Emergency Preparedness

- On the basis of threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits; develop a comprehensive Security Plan, Emergency Response Plan, and Business Continuity Plan that include:
  - Input from public safety and response agencies.
  - Standard operating procedures to cover all potential emergency situations (see Section 3: Threats and Hazards) as well as procedures for dealing with multiple events (e.g., explosive attack and loss of electrical power).
  - An identification of security responsibilities and a chain-of-command in an incident, including roles, responsibilities, and phone numbers for decision makers.
  - An identification of stakeholders that includes tenants, owners, corporate management, insurance carriers.
  - Operations Security procedures to cover routine security activities by all employees.

  - Procedures for dealing with people with special needs (e.g., with physical disabilities or limited English proficiency) Consider FEMA's *Comprehensive Preparedness Guide 301: Interim Emergency Planning Guide for Special Needs Populations* – *http://www.diversitypreparedness.org/Topic/Subtopic/Record-Detail/18/audienceid--15869/resourceid--17720/*.
  - Establish tenant-based life safety teams by floor.

- Review, test, and update all plans as needed throughout the year.
- Register and monitor local alert systems and listservs. Many cities maintain alert systems that allow the jurisdiction to contact users during an emergency by sending text messages to your mobile devices via text or social media. For industry or national threat information, see section 6: Key Federal Protective Programs for instructions to register for NTAS and the Homeland Security Information Network – Critical Infrastructure. For industry-specific threat information, see Appendix C: Additional Resources – Web Sites to register for the Real Estate Roundtable's Real Estate Information Sharing and Analysis Center (ISAC).
- Establish a location within the building for an Emergency Operations Center or Command Center in order to manage the safety and security aspects of the building and its activities during an incident.

  - Ensure the center has adequate resources to conduct emergency operations, including, but not limited to, communications equipment, televisions, office supplies, and computers.
  - Designate a backup location in the event the emergency operations center is disabled.
  - Consider the use of a mobile command center.

- Connect with Local Emergency Planning Committees that exist in accordance with the provisions of the Community Right to Know Act of 1986, or reach out to the local emergency management agency to take advantage of its knowledge base, networks in the community, and planning efforts.
- Share maps of the venue layout (e.g., blue prints, emergency access routes, first aid stations) with local police, fire, and emergency management agencies. In addition, share relevant information, including locations of hazardous materials and fire hydrants. Restrict access to venue data to those public safety agencies and determine how sensitive information will be handled by their agencies. The Department of Homeland Security's Automated Critical Asset Management System (ACAMS) provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel collect and use critical infrastructure asset data, assess critical infrastructure asset vulnerabilities, develop all-hazards incident response and recovery plans, and build public-private partnerships. For more information on ACAMS, see Appendix C: Additional Resources – Web Sites.

- Work with the local emergency medical services for recommendations on how to handle medical emergencies. Consider the following:
  - First aid stations, triage, and transport sites.
  - Emergency routes in and out of the facility.
  - Procedures on what employees are supposed to do in a medical emergency.
- Develop audio and video scripts such as public address announcements for specific emergency announcements, including, but not limited to, natural disasters, weather, bomb threats.
- Have a system in place to maintain accountability for employees, occupants, occupants with special needs, tenants, and contractors.
- Retain copies of the Security Plan, Emergency Response Plan, and supporting documentation in redundant locations. Ensure that key personnel have access to these plans.
- Ensure capability for long-term crisis operations as major incidents can last from several hours to several days.

Security Preparedness

- Develop security plans and procedures to be scalable to the threat of the building. When the threat level is elevated for the building, geographic area, or industry; plans and procedures should provide options for increasing the building's security posture. In addition, establish procedures for returning to lower security levels as the threat decreases.
- Conduct training exercises with building employees, contractors, and occupants to practice the security and emergency response plans to ensure there are adequate resources available to implement the plan, and that all building operation units can implement their responsibilities under the plan.
- Conduct training exercises with law enforcement and emergency responders to familiarize them with the building and its security and emergency procedures. Consider volunteering the building as an after-hours training ground for local emergency response agencies.
- Include neighboring buildings in training exercises to extend knowledge and outreach should emergencies occur.
- Conduct after-action reviews for exercises and revise procedures, as needed.
- Restrict access to sensitive facility data and information (e.g., building plans) and critical items (e.g., specialized equipment), or relocate to areas of the building with greater physical security.
- Develop procedures for shutting down the building in the event the threat is deemed too serious to continue operations.
- Keep records of all security-related incidents and review regularly to identify patterns and trends. Develop procedures for dealing with hoaxes and false alarms so they will not impact building operations.

- Maintain "good housekeeping" practices to reduce the possibility that suspicious items may be left behind and unnoticed, such as:
  - Ensure that landscaping and external aesthetics, trash cans, and mailboxes do not provide hiding places.
  - Keep public, communal, and external areas as clean and well lit as possible, particularly exits, entrances, reception areas, restrooms, stairs, and hallways.
  - Place trash receptacles as far away from the building as possible.
  - Secure dumpsters and other trash receptacles to prevent the hiding of explosives or other hazardous materials; and to prevent unauthorized access to discarded papers and records.

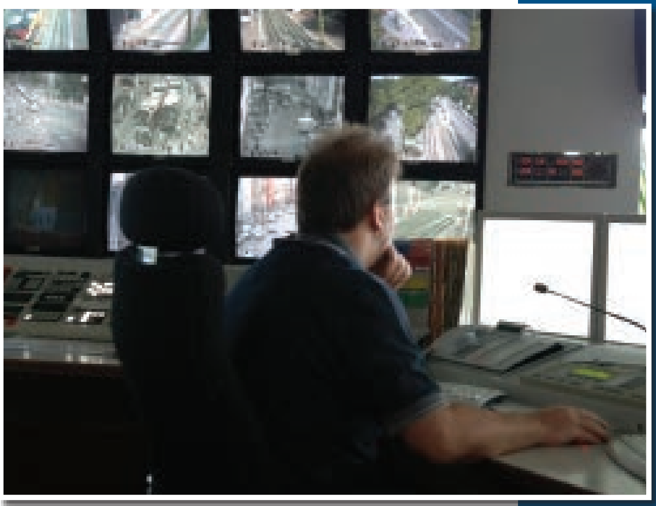
In the event of an elevated or imminent threat:

- Review and implement actions specified in the security, emergency response, and business continuity plans and adjust as necessary to address specific threat information.
- Activate building emergency operations center as appropriate.
- Review threat information to determine whether the building should be evacuated or occupants should shelter in place; operate with limited access, reduced hours, workforce, or activities; or close until further notice. If the determination is to close the building, establish a criteria for when the building should be reopened or restored to full operation.
- Ensure one or more building management employees and a senior security official who are familiar with the plans are available at all times. Maintain an emergency contact list of essential building management personnel, local law enforcement, and emergency services.
- Communicate plans to tenants to ensure plans and procedures are understood by the tenant population in case of an elevated or imminent threat.

4.2 Incident Management

In the event the venue needs to respond to an incident, prepare by considering the following measures:

- Review, test, and update all plans, including the emergency response plan, business continuity, and security plans; ready teams; and incident notification and communication processes.
- Ensure that there are backup personnel who can execute emergency functions if primary personnel are unavailable or incapacitated.
- Ensure that crisis teams can be scaled to fit the situation (e.g., small teams for small incidents, large teams for large incidents).



- Maintain a list of specialized responders with phone numbers and other information. Include persons who speak foreign languages, crane and high-reach equipment companies, and other emergency responders.
- Maintain an emergency shutdown list for water and power. Outline procedures for isolating potential contaminants from the rest of the building. An emergency shutdown capability should be available at all times.
- Review incident command procedures and be prepared to activate a unified command plan with local law enforcement, emergency responders, and other government agencies. Ensure that local law enforcement personnel and emergency responders have access to contact information for the building's security and crisis management teams.
- Determine who will staff the emergency operations center prior to activation. Staffing may include: a security director, potential incident commander(s), fire fighter/EMS personnel, police, building management (operations and security), and private security. Ensure that everyone working within the emergency command center understands the protocols and resulting chain of command for handing an issue over to the appropriate government/public safety authority.
- Ensure that equipment and supplies are available and check their status regularly. The check list should include:
  - Storing emergency supply kits in areas where they are accessible to employees or emergency responders.
  - Determining the need for personal protective equipment for employees (e.g., breathing apparatus).
  - Inspecting the status of all equipment and supplies on a regular basis, for example batteries, flashlights/glow sticks, fire extinguishers, first aid/supply kits, emergency vests, rope, battery-operated radios, masks, and master keys.
  - Maintaining an inventory of long-lead-time and/or specialized equipment and supplies that can be readily available for deployment after an incident (e.g., cleaning agents in the event of a pandemic or public health emergency). Confirm with vendors items to hold on behalf of your property.
- Know the State and local government procedures for obtaining access credentials for off-site building personnel to gain access to the building or affected area in the event of an incident that may restrict access. Develop a list of key personnel who can be pre-credentialed to gain access to the building after an incident. Communicate with local first responders your building's access protocols.
- Develop procedures for building evacuation and shelter-in-place (SIP) situations, including who has the authority to give the order and what emergency situations necessitate which response.
  - For SIP situations, confirm that the tenant organizations have reviewed, discussed, and identified a shelter-in-place procedure within its leased space. (For more information on SIP resources, see the All-Hazards Consortium in Appendix C: Additional Resources – Web Sites.)

  - For SIP situations, maintain stock of non-perishable food, portable water, and emergency supplies to accommodate the number of occupants who may require it to the extent space and leasing considerations allow.
  - Identify an assembly site, and alternate assembly sites where personnel can gather for "head counts" after an evacuation.
  - Identify alternate transportation routes for building personnel to use during evacuations. Test the routes with drills and exercises.
  - For temporary evacuation situations, develop procedures to address readmission of occupants.

- Identify entry and exit points to be used in emergencies. Ensure they are free of obstructions. Refresh staff on these locations and designate staff to guide responders onsite.
- Move objects that could become projectiles (e.g., trash containers, crates, and loose items not attached to a building or to the ground) a safe distance from the building and areas where a large number of people would congregate.
- Update communication templates for media, general public, and stakeholder communications.
- Ensure that additional copies of essential items such as floor plans are kept offsite.
- Consider maintaining an activity log which can capture events as they occur. Designate an employee to maintain and ensure accuracy of the log.
- Maintain a record of security-related incidents. Review regularly to identify patterns or trends.
- Implement procedure for capturing lessons learned and revising response plans after an incident.
- Encourage employees to participate in emergency preparedness and response training sponsored by their community and other outside organizations.
- Develop plans to provide counseling for incident stress management, psychological services, and family assistance for employees in the aftermath of an incident. (For more information, see the American Red Cross in Appendix C: Additional Resources – Web Sites.)
- Ensure that sufficient records and staff are available to manage the insurance recovery process.

In the event of an elevated or imminent threat:

- Review and implement actions specified in the security, emergency response, and business continuity plans; adjust as necessary to deal with specific threat information.
- Pre-position emergency response personnel and equipment to enable rapid response.
- Activate building emergency operations center as appropriate.
- Review threat information to determine whether the building should be closed or operate with reduced hours, work force, or activities. If the determination is to close the

building, evaluate criteria for when the building should be reopened or restored to full operation.

- Ensure one or more building management employees are familiar with the plans, including a senior security official, are available at all times. Maintain contact lists of persons to contact in an emergency.
- Confirm that tenants and occupants understand the plans and procedure to be followed during periods of elevated or imminent threat.

4.3 Personnel

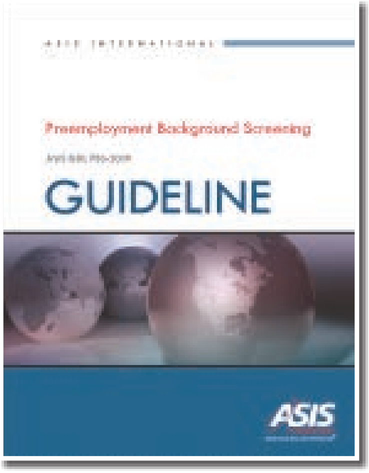
Trained and attentive staff members are an essential element of a successful protective measures program. Employees, contractors (parking, cleaners, building security, etc.), tenants, neighbors, and volunteers should be encouraged to be alert to suspicious activity and out-of-place items. Emphasize the fact that security is a responsibility for all occupants of a building, not merely for security staff, and make it easy for personnel to raise concerns and to report their observations.

A trained building community is essential to ensuring that appropriate actions are carried out in the event of an emergency. Staff should also be trained to remain calm as occupants will look to them for guidance in an emergency.

Hiring a competent and credible staff is just as important to protecting a building as providing staff training. As laws vary from State to State, consider conducting the maximum measures for background checks allowed by State law, particularly in hiring for sensitive positions.

Employees

- Conduct background checks on all employees. Conduct more detailed checks on those who will have access to critical assets, restricted areas, or hazardous materials. Develop a list of disqualifying factors that can be used to reject an individual for employment. Consider verifying identity, employment history, criminal convictions, financial history, and history of overseas criminal activity.
  - The U.S. Citizen and Immigration Services' E-Verify[24] is an Internet-based system that allows businesses to determine the eligibility of their employees to work in the United States. (For more information, see Appendix C: Additional Resources – Web Sites).
  - The *ASIS International Preemployment Background Screening Guideline*[25] is a resource that aids U.S. employers in

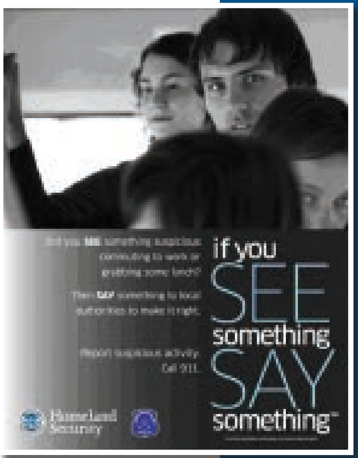


[24] http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=75bce2e261405110VgnVCM1000004718190aRCRD&vgnextchannel=75bce2e261405110VgnVCM1000004718190aRCRD, (accessed June 28, 2013)

[25] http://www.asisonline.org/guidelines/published.htm, (accessed June 28, 2013)

understanding and implementing the fundamental concepts, methodologies, and related legal issues associated with preemployment screening of job applicants and is available for purchase online.

- Establish a threat assessment team to evaluate ongoing personnel risks. Create policies related to recognizing and dealing with personnel in distress.
- Provide safety and security briefings to all staff. Incorporate security awareness and appropriate response procedures for security situations into employee training programs. Include the following in the training.


Did you SEE something suspicious commuting to work or grabbing some lunch?
Then SAY something to local authorities to make it right.
Report suspicious activity. Call 911.
Homeland Security
if you SEE something SAY something™

  - Maintaining alertness to and recognizing situations that may pose a security threat or an indicator of a potential terrorist attack, such as:
    - Suspicious behaviors
    - Persons carrying unusual packages
    - Persons without proper employee identification
    - Unattended or suspicious vehicles
    - Persons parking, standing, or loitering in the same area over a multiple-day period
    - Persons questioning building employees about facility operations and security routines
    - Significant interest being taken near entrances, parking areas, and surveillance cameras
    - Strange odors or liquids
    - Suspicious photography of building and surrounding activities
  - Contact and notification protocols for emergencies and suspicious situations; contact information for all staff should be easily accessible.
  - Caution in providing building information to outsiders.
  - Procedures to provide for the safety of occupants (building staff and tenants) during a security incident including searches, emergencies, and evacuations.
  - Appropriate actions to take in the event of a bomb threat. Provide checklist and train employees who normally answer the phone on how to deal with a phone threat. (See Appendix B: DHS Bomb Threat Checklist.)
- Train all employees on suspicious activity reporting. Consider incorporating information from the DHS "If You See Something, Say Something"™ campaign[26] into training. This campaign is intended to raise public awareness of potential indicators of acts of terrorism, crime, and other threats to the homeland. The nationwide campaign emphasizes the importance of reporting suspicious activity to the proper law enforcement authorities.
- Maintain up-to-date security training with refresher courses. Maintain records of employee training that has been completed.

[26] http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm, (accessed June 28, 2013).

- Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., irregular work hours, attempting to access restricted areas, carrying unusual packages). Maintain an awareness of any unusual patterns of employee illness that might indicate exposure to a toxic agent.
- Review personnel files of recently terminated employees to determine if they pose a security risk.

Security Staff

- Maintain an adequately sized, equipped, and trained security staff based on the threat to your building. Ensure that an appropriate number of security personnel are on duty or on call in the event of an incident. Determine the availability of security staff reinforcements that would be deployed during heightened threat conditions or in response to an incident. Conduct background checks on all security personnel. Some physical security providers are SAFETY Act-certified. For more information on the SAFETY ACT, see section 6: Key Federal Protective Programs.
- Coordinate security staff operations with local law enforcement and, as needed, with State and Federal agencies such as the FBI, DHS (Protective Security Advisor), and fusion centers.
- Develop a security force patrol schedule that includes both regular and random stops and timing.
- Provide additional security measures (e.g., personal security specialists) or bolster existing security measures when hosting high-profile events or when high-profile individuals visit the building. Coordinate plans and communication procedures to ensure safe arrival, attendance, interviews, and departure for special guests. This may involve working with Federal and State protection authorities.
- Develop a procedure for questioning persons acting suspiciously and/or violating security regulations. Train security personnel in appropriate methods for handling these types of situations, identifying sensitive items, and prohibiting their entry.
- Conduct regular training drills and exercises with security staff, building staff, and contractors in coordination with local, State, and Federal law enforcement and emergency management authorities.
- Develop a security staff schedule that includes random patrols of the building and perimeter.

Tenants, Contractors, Vendors, Temporary Employees

- Provide security information and emergency response training to all non-employees who regularly visit the building, including contractors, vendors, and temporary employees. Advise them to be alert to suspicious activity or items, and instruct them on how to report such incidents. Provide instructions outlined in the preceding section for employees on response procedures, as appropriate. Conduct background checks on all security personnel. Some physical security providers are SAFETY Act-certified. For more information on the SAFETY ACT, see section 6: Key Federal Protective Programs.

- Require contractors, vendors, concessionaires, and temporary employment agencies to certify that their personnel meet the security and background standards that are required by their contracts.
- Engage and educate the building's leasing department in its role in building security. Generally, commercial real estate is leased to established companies that occupy a significant amount of space on a floor or multiple floors. Determine the building's leasing rules regarding subtenants who pay a fee to the main tenant, but are not otherwise vetted by building management. This includes tenants whose core business is to sublease areas of their space or administrative staff to small or unknown start-up companies and operations.

In the event of an elevated or imminent threat:

- Update employees, occupants, and vendors about the change in threat status and security situation. Provide refreshers on Standard Operating Procedures (SOPs) to be used in different types of scenarios.
- Increase security staff presence by using additional personnel or overtime. Increase patrols of remote parts of the building and perimeter. Consider augmenting security with special units (e.g., armed guard, K-9 units) and request support from law enforcement personnel.
- If necessary, request additional security staff support from local law enforcement and, as a deterrent, request they post themselves and their vehicles at entrances where they are visible to people entering the building.
- Have employees working in remote or isolated areas of the building work in pairs.
- Have employees vary their routines to avoid predictability.
- Limit noncritical travel and business activity outside the building.

4.4 Physical Security Systems

Physical security systems and access control measures can pertain to the physical access to a building by employees, occupants, contractors, vendors, temporary employees, vehicles, mail, and other deliveries. Measures will vary considerably by the type of building, but can include:

General Measures

- Define the perimeter and areas within the venue that require access control for pedestrians and vehicles.
- Identify especially sensitive or critical areas (e.g., processing areas, control rooms,

communications centers, computer server rooms, shipping areas, mail rooms, fuel or chemical storage tanks and utility access points/service areas) that require special access controls. Where possible, locate sensitive equipment and assets in the interior of the building, and consider installing Closed-Circuit Television (CCTV) and access control systems.

- Evaluate the need/adequacy of perimeter barriers (e.g., fences, walls). Install alarms, intrusion-detection equipment, and CCTV at unstaffed perimeter barriers.
- Maintain the minimum number of access points needed to meet operational and safety requirements. Where necessary, design layered access points that provide multiple opportunities to permit or deny entry. Evaluate and select access control measures for each access point.
- Provide security guards at key access points. Train guards to identify pedestrians and vehicles that are permitted access. Train guards on procedures for denying access.
- Prohibit entry of security-sensitive items (e.g., firearms, explosives, illegal drugs, cameras).
- Enforce all access control measures on a continuing basis (e.g., employee bag check, locking of rooms not in use) on a continuing basis. Allow no exceptions. Implement rigorous key control procedures. Secure master keys. Secure all tools that could be used to force entry into a critical area (e.g., bolt cutters, hacksaws, cutting torches).

- Regularly inspect and test all access control devices (e.g., electronic key readers).
- Identify a "buffer zone" extending out from the building perimeter that can be used to further restrict access to the venue when necessary. Coordinate with local law enforcement on access control measures that can be used in this area.
- Consider approaching neighboring facilities to install CCTV equipment in locations which will display exterior images of the facility and reciprocate with neighboring facilities.
- Maintain clear areas at the building's perimeter or perimeter barriers (i.e., keep the areas free of vegetation) to allow for continuous monitoring and to inhibit concealment of people or packages. Inspect the perimeter regularly.
- Coordinate with local agencies to establish and understand emergency access lanes for fire, police, and EMS personnel, as well as mustering areas where police and fire will establish Incident Command posts. Allow emergency services vehicles to be parked near entrance points and near critical assets or areas to ensure timely response to an incident.

Employees and Occupants

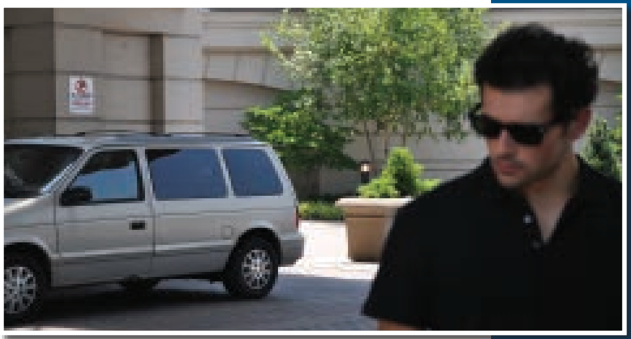
- Issue photo identification badges to employees. Require that badges be displayed and verified to gain access to the building, and worn at all times inside the facility. See section 4.5 – Credentialing.
- As necessary, issue special employee badges to authorize access to sensitive areas.

Utilize an electronic access tracking system to log entry and exit from the venue and/or sensitive areas.

- Develop a policy for off-duty personnel accessing sensitive areas.
- Develop a policy for lost employee identification badges for building staff and tenants.
- Practice the staff employee response to any person without a badge in a restricted area of the venue.
- Collect employee identification and keys when a person is no longer employed at the facility. Consider changing locks, combinations, or codes.

Contractors, Vendors, Temporary Employees, and Visitors

- Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees. Require that badges be displayed at all times and verified to gain access to the building. Collect all badges when visits are complete.
- Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement. Require sign-in and sign-out of contractors, vendors, and temporary employees.
- Consider signing out a communication device (i.e., two-way radio) to contractors to improve communications during an emergency situation.
- Encourage employees to develop a familiarity with contractors, vendors, and temporary employees. Have them question any unusual or unfamiliar people and report incidents to facility security personnel.
- Escort all non-employees (e.g., cleaning crews) in sensitive or critical areas. Escort maintenance workers throughout their service visit and visually inspect their work before final acceptance of service.
- Review all requests for visitor access, tours, demonstrations, and displays. If possible, screen visitor requests with local law enforcement to identify potential problems.
- Require sign-in/sign-out for visitors and issue them special identification badges.
- Require that badges be displayed and verified to gain access to the facility. Require that badges be worn at all times in the facility.
- Limit access to visitors or customers to a level consistent with facility operations. Have security personnel deny access to anyone displaying suspicious behavior.
- Where possible, maintain a regular list of customers, vendors, delivery personnel, and other regular visitors.
- Assess the need for checking personal items, such as bags, when coming into or leaving the building.
- Require that contractors who have completed their work return all keys.

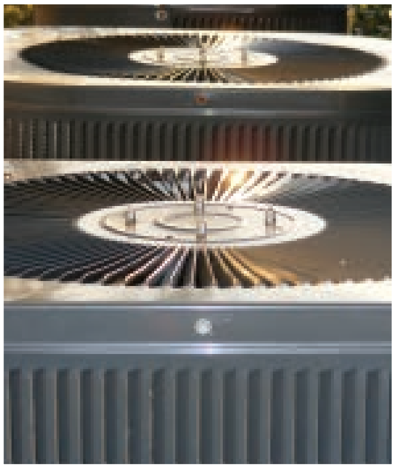


Vehicles and Parking

- Review vehicle traffic patterns around and inside the building. Design and implement traffic-control strategies and barriers (e.g., road alignment, serpentine traffic routine, swing gates, speed bumps) to control vehicle speed and approaches to critical assets and places where crowds congregate.
- Locate general parking in areas that present the fewest security risks to personnel. To the extent possible, keep vehicles distant from areas where large numbers of people congregate.
- If possible, review parking beneath or within a building. If parking beneath a building is unavoidable, limit access to the parking areas and ensure they are secure, well-lit, and free of places of concealment.
- Positively identify vehicles and drivers that enter the building and consider applying the following restrictions:
  - Public parking with ID check (where practical)
  - Company vehicles and employees of the building only
  - Selected company employees only, or those requiring security
- Deny access to suspicious vehicles, vehicles and drivers with improper documentation, or those who refuse to provide identification or submit to inspection. Assess whether vehicles need to be searched before being allowed access to the building. Develop inspection criteria.
- Maintain a database of employee-owned vehicles and issue parking permits for designated areas of the premises. Limit vehicle access to sensitive or critical areas to those who have been positively identified, whose vehicle has been inspected, and who have a definite need to be in the area.
- Consider using centralized parking and shuttle bus service to keep vehicles away from large groups of people and critical assets. Identify drop-off points for shuttle buses that are not immediately adjacent to entrance areas where crowds may gather.
- Maintain a log of all vehicles entering the premises (see also *Mail, Shipment, Deliveries* section).
- Lock building service vehicles when not in use.
- Determine who should approach illegally parked vehicles and provide training for those persons to best protect themselves and the public in this situation. Require that the vehicles be moved or have them towed.

Critical Rooms, Shipping/Receiving Areas, Storage Facilities, and Utility Access

- If appropriate, install interior building barriers (e.g., locked doors, walls) to protect sensitive or critical rooms and corridors.
- Provide adequate door and window locks, barred entryways, fencing and gate locks, timed closure devices, and other access controls to buildings, rooms, elevators, shipping/receiving areas, storage tanks and bins, utility access points (e.g., utility



tunnels, manholes), hazardous materials (e.g., fuels, chemicals), and other areas where access is to be limited. Add intrusion detection systems and alarms as appropriate.

- Prevent contamination to the entire building by deterring and blocking access to the ventilation system. Install controls for barriers to HVAC systems (e.g., intake screens, filters) to prevent the introduction of chemical, biological, or radiological agents into the building. Where needed, provide positive pressure in the building to prevent contaminants from entering. Train staff in emergency HVAC system shut-off procedures.
- Utilize stronger security controls such as card swipe locks in sensitive or critical areas of buildings. Use an electronic access tracking system to log entries and exits from critical facilities.
- Provide additional security to buildings and other assets that are on the site perimeter where they may be more open to attempts at unauthorized entry.
- Provide security to ladders, awnings, and parapets that give access to building roofs, HVAC systems, and other critical equipment. Ensure that nearby foliage (e.g., trees, shrubs) cannot be used to gain access to the building's roofs.
- Lock and secure rooms or assets when not in use. Ensure that all areas containing equipment used by the security force (e.g., communications gear, uniforms, weapons) are locked and secured.
- Document areas within the building where Uninterruptible Power Supply (UPS), batteries, and storage of chemicals exist, inform local first responders of their locations, and confirm any special needs these groups may have.

Mail, Shipment, Deliveries

- If possible, screen all deliveries to the building, including U.S. mail and commercial delivery services.
- Accept deliveries and shipments only from known shippers, vendors, or customers. Maintain a log of all vehicles entering the premises.
- Train mail room and receiving personnel to recognize suspicious mail or deliveries. (See Appendix A: Suspicious Mail or Packages and Appendix C: Additional Resources – Web Sites.)
- Designate an area for processing mail that is separate from central ventilation.
- Limit delivery times. Schedule as many deliveries as possible for times when the building is not open to the public, such as the early morning. When this is not possible, ensure that practices and protocols for how to respond to emergency situations involving suspicious packages are understood by building personnel.

- Consider requiring that delivery vehicle drivers, helpers, and passengers produce a photo ID and sign in at a designated control point.
- Reserve the right to inspect or reject any delivery.
- Consider escorting delivery vehicles to the area near or within the building where the delivery is made when applicable.

In the event of an elevated or imminent threat:

- Communicate with tenants and occupants the procedures to be following during elevated or imminent threats.
- Reduce the number of access points for pedestrians and vehicles. Increase the security (e.g., additional guards and inspections) at each open access point. Consider closing the building until the threat has been reduced.
- Reduce access to the building to a minimum. Delay or halt non-essential contractor work and escort essential contractors and vendors while on the premises. Close building access to visitors.
- Consult with local authorities about restricting access to the buffer zone around the building. Evaluate the need for closing or restricting traffic on nearby roads, waterway, or public access areas adjacent to the building. Increase the number and security level of barriers to the maximum extent possible that is consistent with the operating level of the facility.
- Deploy temporary barriers (e.g., Jersey barriers, heavy vehicles and equipment, empty containers) to increase the standoff distances from critical areas and to slow the flow of traffic into and within the building.
- Restrict parking to areas away from critical assets. Evaluate the closure of associated underground or under-building parking lots.
- Tow illegally parked vehicles and vehicles in authorized spaces.
- Redirect mail, shipments, and deliveries to areas distant from sensitive or critical assets. Accept deliveries only during daytime hours.
- Require that employee badges be worn at all times in the building.
- Review available threat information and consult with law enforcement authorities to determine if the building should be closed. If the determination is to close the building, evaluate criteria for when the building should be reopened or restored to full operation.

4.5 Credentialing

Credentialing procedures offer the means to identify key personnel within a building, as well as control access. Credentialing options may range from electronic badges used in venues to colored shirts, smocks, and hats worn by volunteers at events. Consider the following credentialing measures:

- Issue photo identification badges to all employees. Require that badges be displayed and verified to gain access to the building, and worn at all times inside the facility. Occasionally, test the response of employees to unauthorized persons at the building. As necessary, issue special employee badges to authorize access to sensitive areas. Utilize an electronic access tracking system to log entry and exit from the building and sensitive areas.
- Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees. Require that badges be displayed at all times and verified to gain access to the building. Collect all badges when visits are complete.
- Devise credentialing systems that indicate permissions, to include:
  - Areas of access (e.g., utility and mechanical areas)
  - Purpose of activity on the premises (e.g., maintenance)
- Consider color-coding the credentials for easier identification.
- For buildings or campuses with fixed gates and fences, consider requiring that employees swipe badges before entering the premises.
- Require written requests for credentials prior to entry (including media). Require that those designated to pick up credentials do so in person using photo identification.
- Maintain a record of people who are issued credentials.
- Ensure all employees, media members, and vendors wear credentials issued by building management.
- Train access control personnel in credential recognition. Instruct them to deny access to those not displaying the appropriate credentials. Display credential boards/ access documentation at access control points or provide personnel with sheets/cards displaying the different credentials.
- Develop procedures for reporting and replacing lost or stolen credentials, including denying access to the barcode, if applicable. Require that credentials be returned as part of the out-processing procedures when employees no longer work at the building. Individuals who do not return credentials should be identified and those credentials should be deactivated.
- Implement a policy that addresses off-duty personnel accessing sensitive areas.
- Consider the use of a license reader and photo identification to document the individuals given access to the facility.
- Conduct regular badge audits to confirm active badges.

In the event of an elevated or imminent threat:

- Require that employee badges be worn at all times in the building.

WARNING
Hazardous Voltage Inside
Keep Out !
Authorized Personnel Only
High Voltage equipment inside can shock and burn.

4.6 Signage and Notification

Signage and notification are essential to convey important information to employees, occupants, and visitors to buildings. The signage protective measures described below should be considered for use by buildings:

- Post signage relating to emergency ingress and egress routes, first-aid stations, and shelters.
- Use signage (e.g., electronic signage, posters on easels) to instruct visitors on what to do in the event of severe weather and emergency situations.
- Establish a "Security Awareness Campaign" through information provided on the venue's Web site, mailings, and signage to encourage employees and occupants to report suspicious activity to the nearest building staff, security officer, or law enforcement officer.
- Ensure signage clearly identifies the types of access permitted through specific areas of the building. Signage is also recommended for directing delivery trucks to their appropriate destination and checkpoint.
- Provide appropriate signage to identify access points and areas with restricted access. Signs may clarify restricted access; however, refrain from identifying sensitive areas with signage including those with critical utilities.
- Consider signs with multiple languages where necessary.

In the event of an elevated or imminent threat:

- Use additional signage (e.g., electronic signage, posters on easels) to provide a simple and straightforward means for people to communicate the presence of a potential threat or an emergency.

4.7 Barriers

The use of physical barriers and controls can serve a variety of purposes at a building. Barriers can designate a space or provide legal boundaries for a property, control the entry and traffic flow of both pedestrians and vehicles, provide a standoff distance from explosives, and potentially deter hostile surveillance and unauthorized access. Barriers can be temporary or permanent, natural (e.g., rivers, waterways, steep terrain, and plants) or manmade (e.g., fencing, walls, bollards, planters, and concrete barriers). The use of barriers – and their regular inspection by security – can create a secure environment that balances the operational, security, and aesthetic interests of a building. For additional information, FEMA 430: *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*[27] provides information and design concepts for the protection of buildings and occupants, from site perimeters to the faces of buildings.

[27] http://www.fema.gov/library/viewRecord.do?id=3135 (accessed June 28, 2013).

Perimeter Barriers

- Locate the perimeter, the outermost line that can be protected by security measures, as far as practical from the building exterior.
- Evaluate the need for perimeter barriers around the building (e.g., fences, berms, concrete walls). Consider natural features (e.g., hills, woods, waterways) that could either enhance or inhibit security at the facility.
- If appropriate, install perimeter barriers (e.g., remotely closed gates). Maintain a clear area at perimeter barriers to enable continuous monitoring and to inhibit concealment of people or packages. Inspect perimeter barriers regularly.
- Consider installing alarms and intrusion-detection equipment at perimeter barriers.
- Post appropriate signage (e.g., no trespassing, restricted access, site is monitored, no parking).

Building Barriers

- In a campus environment, establish clear zones adjacent to sensitive or critical buildings. Keep zones free of obstructions to allow for continuous monitoring and to inhibit concealment of people or packages.
- If appropriate, install individual building perimeter barriers (e.g., fences, bollards, decorative flowerpots, high curbs, and shallow ditches) around sensitive or critical buildings. Consider the requirements for fire protection and emergency vehicle access in the design of building perimeter barriers.
- Install secure barriers around HVAC systems (e.g., screens on intakes, filters) to prevent the introduction of chemical, biological, or radiological agents into any buildings on the premises. (Train staff in emergency HVAC system shutoff procedures.)

- Consider protective options that will mitigate the effects of small arms firing and explosive blasts (e.g., anti-shatter film, glazing protection, blast-resistant and shatter-resistant glass, offset entryways, shrubbery), as many of the casualties in terrorist attacks are caused by flying glass, especially in modern buildings.
- Move objects that could become projectiles (e.g., trash containers, crates, construction materials, loose items not attached to a building or to the ground) a safe distance from buildings and areas where large numbers of people congregate. Locate trash containers in well-lit areas where they can be observed by security cameras. Place containers away from sources of secondary fragmentation, such as windows, mirrors, or overhead glass. Use blast-resistant trash containers and transparent container liners.
- Ensure exterior door hardware is resistant to tampering (e.g., chained shut). Ensure exterior doors have hinge pins that cannot be removed from the outside and that there are no gaps between the door and jamb that would allow for the door to be compromised.

- Ensure that the building has smoke-proof stairways and exit corridors that can be used for evacuation.
- If appropriate, install interior building barriers (e.g., internal locked doors) to protect sensitive and critical areas or corridors within a building.

Vehicle Barriers

- Evaluate vehicle traffic patterns around and within the building. Design and implement traffic control strategies and barriers (e.g., road alignment, serpentine traffic routing, retractable bollards, swing gates, speed bumps) to control vehicle speed and approaches to sensitive or critical assets.
- Install crash-rated vehicle barriers where practical (e.g., bollards, surface mount plate barriers, drum barriers, gate barriers) to keep vehicles a safe distance from buildings and areas where people congregate.
- Install removable bollards on pedestrian walkways to keep unauthorized vehicles off walkways.

In the event of an elevated or imminent threat:

- Increase the number and security level of the barriers to the maximum extent possible that is consistent with the operating level of the building. Deploy temporary barriers (e.g., bollards, Jersey barriers, heavy vehicles, and equipment) to increase standoff distances from the building, and to provide additional traffic flow and access control.
- Deny access of vehicles onto the premises by stopping them at the property perimeter access point. Deploy redundant barrier controls to enable vehicle screening to be temporarily undertaken at a location that is a maximum safe distance from the property.
- Incorporate a secure shuttle service for guest transportation to and from the perimeter vehicle screening point.
- Incorporate a secure escort process for service deliveries from the perimeter vehicle screening point to the loading dock or drop-off point.
- Relocate sensitive or critical items (e.g., specialized equipment, vital records) to areas of the building with higher physical security.

4.8 Communication, Networking, and Notification

Communication protective measures for a building can encompass equipment, protocols, and information sharing, including the following:

General Measures

- Develop a communication and notification plan that covers voice, data, and video transfer of information related to safety and security. Provide a simple and straightforward means for people to communicate the presence of a potential threat or emergency.

Communications Equipment

- Install communications systems (e.g., mass notification, public address, cell phones, pagers, panic buttons) that can reach all building occupants, notify them of threats, and provide emergency procedures. Urge recipients of emergency messages to inform others. Test often.

- Provide redundant communication channels (e.g., telephone, radio, pager, public address system) that can be used in the event that one channel is disabled. Provide backup electric power (e.g., uninterruptable power supplies, backup generators) to run communications systems.
- Ensure that there are procedures and equipment for communicating with local law enforcement and emergency responders.
- Have emergency communication equipment (e.g., cell phones, emergency radios) available for use in the event that all primary channels are unavailable.
- Test all systems and equipment regularly and train employees in the use of the communication systems.
- Consider installation of a priority access communication system to allow access to preferred users involved in emergency management.
- Provide communication security (e.g., encryption, multiple frequencies, countermeasures sweeps) that will prevent unauthorized interception of information being transferred.
- Consider installation of a special panic alarm system in sensitive or critical areas.
- Provide the ability to record incoming communications (e.g., telephone calls) to identify and document potential threats.
- Coordinate with communication service providers (e.g., telecommunications companies) on plans and procedures for restoring service in the event of a disruption.

Communications Protocols

- Develop a communication and notification plan that covers voice, data, and video transfer of information related to security.
- Develop a notification protocol that outlines who should be contacted in emergencies. Designate who is to contact whom within the building, both building management and tenants, and with outside organizations. Provide a contact list to all who might need it and keep the list up-to-date. Test the notification protocol through drills and exercises.
- Develop a process for communicating to employees and occupants the security situation and reminding them of steps that should be taken in the event of an incident.

Keep security advisories up-to-date as the situation changes. Develop a process for communicating this information to off-duty building staff.

- Develop a system to account for employees, tenants, and contractors. Ensure the information can be accessed offsite in the event of an emergency.
- Provide a simple and straightforward means for people to communicate the presence of a threat or an emergency (e.g., hotline number, internal 9-1-1 capability). Develop a process to warn occupants of criminal activity in and around the building.
- Consider a contact information checklist to include owners, staff, tenants, law enforcement, other government agencies, hospitals, insurance providers, neighboring facilities, and emergency service contracts. For emergency service contact information checklists, include vendors in charge of electrical, Information Technology (IT), elevators, generators, HAZMAT, HVAC, plumbing, sewage, and language translation.
- Take steps to restrict the release of information that might compromise the security posture of the building. Train employees not to discuss sensitive information over communications channels that are not secure (e.g., cell phones).
- Develop a process for communicating with the public and the media regarding security issues, including the handling of inquiries. Identify the people who will have responsibility for media interactions. Provide adequate information to quell rumors and dispel unnecessary alarm. Provide training on casualty notification.

Information Sharing

- Monitor industry and government information on threats, incidents, and response procedures. The initial report about the building's experiences with suspicious or criminal activity should go to the local law enforcement agency. Additionally, suspicious activity can be reported to State and local fusion centers,[28] as well as reported on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Suspicious Activity Reporting (SAR) Tool. The SAR tool is meant to supplement, not replace, other means of suspicious activity reporting and to share information with your HSIN-CI Community of Interest. See section 6: Key Federal Protective Programs for more information on fusion centers, FBI Joint Terrorism Task Forces,[29] and HSIN-CI.

In the event of an elevated or imminent threat:

- Provide a secure means for security staff to communicate with each other during periods of heightened threat and emergency.
- Increase frequency of communications with local law enforcement. Advise them of the heightened security status at the building. Identify additional security measures that will be implemented.
- Increase communications with employees about the security situation and provide reminders about actions to take in the event of an incident.

[28] The nearest State and local fusion center's contact information can be found on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI). To register for HSIN-CI and the Commercial Facility Community of Interest, email: HSINCI@hq.dhs.gov

[29] The FBI regional phone numbers can be found online at http://www.fbi.gov/contact-us/field.

- Increase the frequency of reporting and call-ins from employees, particularly those in remote areas of the building.
- Test communication equipment, including primary and backup systems frequently. Have backup communication equipment activated and ready for use in the event of an incident.

4.9 Monitoring, Surveillance, and Inspection

These measures relate to procedures and equipment used to monitor the movements of people, vehicles, and materials.

General Measures

- Design a monitoring, surveillance, and inspection program that is consistent with building operations and security requirements. Begin monitoring operations at a standoff distance and continuing monitoring closer to the center of activity. Coordinate your activities with local law enforcement, and maintain awareness of activities in the area surrounding the building.
- Provide visual surveillance capability (e.g., designated surveillance points, cleared lines of site) for sensitive and critical assets at the building. Maintain vigilance and keep surveillance areas clear of obstructions (e.g., vegetation, parked vehicles) that would inhibit observation.
- Monitor work being done adjacent to the building (e.g., road construction, utility equipment servicing) for signs of unusual activities (e.g., planting packages near assets or gathering places).
- Ensure routine security patrols are not predictable. Regularly inspect internal and external areas, including the site perimeter, parking lots, equipment, trash containers, and sensitive or critical areas. Even if there are roving building patrols, individuals may need to be assigned to special areas to prevent theft or tampering.
- Train security staff to identify surveillance techniques including the ability to recognize activities such as suspicious loitering or taking photos of utility systems.
- Coordinate with the local police department on the use of trained and certified dogs to check for explosives or other dangerous items.

- Monitor people entering and leaving the building. Train monitors to recognize suspicious behavior (e.g., unusually bulky clothing that might conceal weapons or unusual packages).
- Monitor the activities of contractors, delivery personnel, and vendors while they are at the building for unusual activities or behavior. Inspect all work before releasing contractors.
- Inspect packages, briefcases, backpacks, parcels, and luggage being carried by people, where practical (e.g., employees, contractors, vendors, and visitors). Inspection may be random, spot check, or comprehensive, and may include hand searches of packages, metal detectors, X-ray scanners, or explosive-sniffing dogs. Provide more thorough inspection for those entering sensitive or critical areas.
- Maintain an awareness of materials already in place at the building that could be leveraged for illicit purposes (e.g., flammable materials, chemicals). Maintain a thorough inventory and accounting of these and other sensitive items; their storage; and movement into, out of, and within the building.
- Use countersurveillance teams and techniques to periodically test the effectiveness of existing systems against emerging threat tactics.

Equipment

- Install and maintain sufficient lighting inside and outside the building.
- Install detector and alarm systems and video surveillance equipment. For detector and alarm systems, include instruction detectors, fire and smoke alarms, motion detectors, CBR material detectors, and explosives detectors as appropriate. For surveillance detection equipment, include CCTV, lighting, and night-vision equipment where indicated by a risk assessment, and interconnect with other detector and alarm systems (e.g., fire, smoke) as appropriate. (Remember that CCTV is only useful if monitored and used properly.) The following practices are helpful when using detector and alarm systems and video surveillance equipment:
  - Provide both centralized and distributed capability to monitor and record detector, alarm, and video feeds. Maximize the recording time.
  - Train personnel to interpret detector and alarm signals and to identify potential security-related events.
  - Review recordings regularly for unusual activities or patterns.
  - Establish procedure to secure detector, alarm, and video recordings for forensic purposes.

  - If appropriate, provide detector, alarm, and video feeds to local law enforcement or other organizations outside of the building.
  - Provide coverage for the building's perimeter, sensitive and critical assets in the building (e.g., labs, HAZMAT centers, data storage, VIP offices), building entrances, parking lots, loading docks, vehicle roadways, and the buffer zone around the building.
  - Train personnel to interpret video and identify potential security-related events. If neighboring facilities employ CCTV, particularly in locations which will display exterior images of your facility, educate neighboring facilities on how to identify potential security-related concerns or events.
- Regularly check emergency/security equipment systems (e.g., sensors, alarms, backup power, lighting).

Vehicles

- Monitor all vehicles approaching the building for signs of threatening or suspicious behavior and be prepared to take defensive action (e.g., engage barriers, deploy security vehicles). Signs of threatening or suspicious behavior in vehicles include, but is not limited to:
  - Unusually high speed
  - Riding particularly low
  - Emitting a chemical odor
  - Occupants keeping the windows open even in cold or inclement weather
  - Erratic driving (fast then slow, swerving, attempting to piggyback, etc.)
- Use random inspections or inspection of all vehicles, as appropriate. Inspection can be brief (e.g., observe passenger compartment of automobiles, open loading door of trucks) or comprehensive (e.g., inspect undercarriage, engine compartment, automobile trunk). Vehicles may be grouped into two classes: trusted (e.g., employee vehicles, company vehicles) and other. Inspections may vary by class.
- Consider current and future inspection technologies (e.g., above vehicle and under vehicle surveillance systems, ion scanning, X-ray equipment, license plate readers).

Deliveries and Mail

- Monitor and verify deliveries and supervise the unloading of materials and equipment to the building:
  - Verify the shipper, driver, delivery manifest, and material being unloaded to ensure conformity to what is expected.
  - Verify that seals on deliveries have not been tampered with.
  - Conduct more thorough inspections for deliveries involving hazardous or sensitive materials.
  - Reject deliveries that fail to conform to requirements.

- Train receiving personnel to recognize suspicious mail, packages, shipments, or deliveries, and instruct them on notification procedure (for more information, see Appendix A: Suspicious Mail or Packages):
  - Inspect all mail for unusual signs such as leaking, powders, strange odors, and no return address.
  - Direct suspicious mail or packages to a controlled area for handling.
  - Provide personnel protective equipment for those handling suspicious mail or packages.
  - Advise employees to check all deliveries and mail at home for suspicious material.
  - Maintain records of all deliveries.

In the event of an elevated or imminent threat:

- Increase monitoring and surveillance of sensitive and critical assets, people, vehicles, materials, and equipment. Reassign personnel to assist in surveillance, monitoring, and inspection duties. Request additional support from local law enforcement as necessary.
- Increase monitoring of video surveillance, alarms, and equipment detectors. Route detector feeds to local law enforcement. Implement continuous monitoring as necessary.
- Install additional temporary lighting to provide increased illumination. If possible, increase lighting in buffer zone as well.
- Increase frequency and thoroughness of inspections of buildings and assets to the maximum level sustainable. Close and secure non-essential areas and assets.
- Search all persons entering the facility. Deploy portable scanning equipment (e.g., metal detectors, X-ray scanners) to increase the level of inspection.
- Restrict what people are permitted to carry into the building. Prohibit packages from being brought into the building.
- Thoroughly inspect all vehicles and deliveries made to the building. Postpone non-essential deliveries. Consider processing deliveries at a remote site. Consider augmenting inspection with special units (e.g., K-9 units).
- Isolate or remove any hazardous materials that might increase the impacts of an attack.
- Consider restricting entry to essential personnel only.

4.10 Information Security and Cybersecurity

Information is crucial to business operations and if lost, damaged, or stolen may affect the security and reputation of an organization. A compromised cyber network has the potential to shut down day-to-day operations and exploit corporate, personal, or financial information. Consider these measures to protect cyber networks, building control systems, and information systems:

Cybersecurity

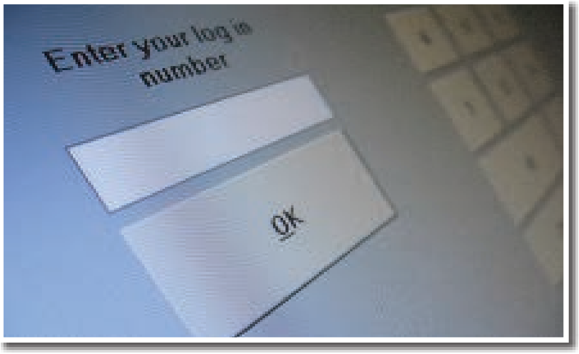
- Develop and implement a security plan for computer and information systems, hardware, and software associated with the building. Design and implement secure computer network architecture and ensure that business and enterprise security policy is followed.
- Maintain a well-trained computer security staff with the appropriate knowledge and experience to manage cyber security issues. To secure specific devices and systems, regularly consult with trade organizations, vendors, or specialists about cybersecurity practices, standards, and strategies.
- Conduct thorough background checks on employees serving as system administrators and have the background checks updated regularly.
- Install and maintain up-to-date cybersecurity techniques (e.g., firewalls, virus protection, spyware protection, encryption, user authentication), software patches, and strategies:
  - Ensure systems and networks have sufficient defense-in-depth mechanisms.
  - Provide audit and forensic capability, with easy tools for detecting inappropriate activity.
  - Ensure critical host computers do not have inappropriate applications (e.g., games) installed.
  - Enforce password procedures (e.g., frequency of change, strength, and password reuse).

  - Provide adequate control over remote access and modems (e.g., land-line and wireless).
  - Back up data and configuration files regularly. Maintain backups in a separate/secure location.
  - Develop redundancy in technology hardware and software to keep critical systems operating. Test these plans and procedures.
  - Monitor computer systems regularly to detect any patterns of probing, hacking, or intrusions.
  - Work with the Internet service provider to implement protective measures against attacks (e.g., denial of service attacks).
  - Stay up to date on the latest cybersecurity threats, incidents, and defensive measures.
  - Regularly test computer security measures (e.g., audits, penetration testing, drills). Test all applications that involve the handling of sensitive information for potential vulnerabilities.
- Control physical access to IT equipment (e.g., computer rooms, payment systems, and surveillance systems). Install locks and access controls to allow only authorized personnel to enter. Provide communication capabilities to allow rapid reporting of incidents.

- Carefully validate the credentials of all contractors and vendors given access to computer systems and ensure that access to systems is on a need-to-know basis.
- Review the building's Web site to ensure it does not contain any sensitive information such as staff contact information, proprietary information, financial information, technical specification, and chemical and biological data. Ensure that the Web site is protected with up-to-date security software.
- Develop an acceptable use policy for staff regarding personal use of work computers such as Internet use, email, and social media.
- Provide training to all employees using computer systems on cybersecurity threats (e.g., email phishing; deceptive inquiries from outsiders; and malicious code such as viruses, worms, and Trojan horses) and measures for protecting the systems. Train employees on cybersecurity responsibilities (e.g., changing passwords regularly, not divulging computer information to others, not opening unknown email attachments).
- Immediately cancel computer access for transferred, retired, or terminated employees. If exit interviews are conducted with employees, ensure this step is part of the exit interview checklist.

Control Systems

- Identify any critical communications, industrial controls (e.g., access control, HVAC, water distribution systems), and information technology systems that support critical building operations and implement cybersecurity defensive technologies to protect them from unauthorized access.
- Form a team arrangement between IT cybersecurity and control systems engineering staff to facilitate effective knowledge sharing and joint security initiatives.
- Implement effective policies, procedures, and culture to govern control system security.
- Limit user accounts with administrative or root privileges. Conduct background checks on employees serving as control system administrators. Require background checks for contractors and validate their credentials and work performed on control systems.
- Regularly consult with trade organizations, vendors, or specialists about control system security, practices, standards, and strategies.
- Install and maintain up-to-date process control security techniques, patches, and processes:
    - Conduct a thorough risk assessment before connecting process control systems to the Internet, before using wireless communications for critical control applications, and before connecting process control systems to business networks that have Internet connectivity. Perform regular network mapping tests to determine if control systems have been unintentionally connected to outside networks, including the Internet, or if malicious actors have adjusted devices to purposely create these connections.



- Deploy firewalls to restrict traffic entering and leaving control networks and between business and control networks. Minimize remote access to control system computers.
- Segregate critical command and control functionality from noncritical traffic and detect and disable inappropriate applications (e.g., games, personal digital assistants, flash drives).
- Implement technology to discover rogue wireless access points and devices. Implement procedures for disabling unintended WiFi-capable equipment connected to critical networks (e.g., laptops introduced into control centers).
- Assure that security processes can detect unauthorized information creation or modification of information, authorized access for unauthorized purpose, packet alteration (e.g., interception, modification, forwarding), and compromises to data confidentiality. Perform regular network mapping tests to determine if control systems have been unintentionally connected to outside networks, including the Internet, or if malicious actors have adjusted devices to purposely create these connections.
- Use intrusion-detection strategies that use anomaly, signature, statistical, and vulnerability attack interception techniques.
- Change factory-default passwords and commonly used passwords and replace them with strong password practices (e.g., frequency of change, strength, and password reuse).
- Explore system protocols that contain appropriate authentication and integrity attributes.
- Establish a robust patch-management process for hardware, firmware, and software.
- Maintain full system backups for critical systems and periodically test procedure for rapid deployment and recovery.

Physical Information Security

- Restrict access to sensitive building data and information (e.g., plans and directories).
- Control all sensitive documents by requiring employees to secure them when not in use. Utilize shredders or a document service to destroy unneeded documents.
- Ensure that copies of security and emergency response plans are protected from unauthorized disclosure.
- Include information security in staff training. Train staff to secure sensitive material, to not leave items lying on desktops, and to log off computers when not in use.
- Laptops and portable equipment should be password protected and never left unattended.
- Erase or overwrite electronic media (e.g., CD-ROM, DVD, USB flash drives).
- Invest in secure cabinets to store sensitive material.
- Keep records of all security-related incidents; review the records regularly to identify patterns and trends.

In the event of an elevated or imminent threat:

- Increase computer security to maximum levels.
- Reduce access to computer systems to the minimum level possible.
- Reduce access to the Internet and other portals that might present a security risk.
- Delay scheduled maintenance and upgrades on software and hardware that is not security-related.
- Increase frequency of system back-ups.
- Increase monitoring for system probes, intrusion, and other anomalies. Advise employees to increase vigilance with regard to unusual computer activities.
- Ensure technical support personnel are available 24/7 to manage any problems.
- Delete information from the Web site that may help potential adversaries plan an attack. If necessary, consider disabling the building Web site.

4.11 Infrastructure Interdependencies

Buildings are complex entities that must rely on utilities, partners, and other infrastructure to continue their day-to-day operations. In addition, many real estate facilities have unique relationships and significant interdependencies with other critical infrastructures, such as Communications, Banking and Finance, Transportation Systems, and Information Technology Sectors, that potentially increase their overall risk. The following protective measures relate to the protection of utilities, including electric power, natural gas, water, telecommunications, and others:

- Ensure that the venue has adequate utility service capacity to meet normal and emergency needs. Identify all utility service points that support the building (from source to site).
- Establish regular communication channels with utility service providers to discuss infrastructure dependencies, review existing systems, capacity expansion needs, and actions to be taken in response to loss of service from primary supply sources and other emergencies. Such providers include, but are not limited to:
    - Electric
    - Gas
    - Water/Discharge
    - IT/Telecommunications
    - Trash Collection
    - Parking/Transportation
    - Damage Restoration/Debris Removal

- Determine, in detail, the physical locations of the following critical support architectures:
  - Communications and Information Technology
  - Utilities (e.g., power, water, natural gas)
  - Lines of communication that provide access to external resources and provide movement of people (e.g., road, rail, and transportation)
- Put utility supply facilities and equipment that are potentially hazardous (e.g., liquid fuel tanks, high-voltage power lines) a safe distance from the building or areas where people congregate. If possible, locate these supplies off site. Monitor the safeguarding of any products and/or chemicals that must be stored onsite, and handle in compliance with State regulations.
- Where practical, provide for redundancy and emergency backup capability for critical utility services (e.g., backup electric power generators, multiple utility feeder lines). Where possible, locate the redundant and backup equipment in a different part of the building than where the primary supply equipment is located. Inspect and maintain backup equipment regularly.
- Ensure employees know how to shut off utility services in emergencies.

- Provide adequate physical security (e.g., fencing, locks, protective enclosures, access restrictions) for utility services, fuel storage containers, trash dumpsters, and HVAC systems. Install special locking devices on utility access points (e.g., manhole covers, HVAC vents).
- Provide for regular monitoring and inspection of utility services (e.g., security patrols, CCTV) and their security measures.
- Develop a decontamination plan (e.g., from Chemical, Biological, and Radiological agents) for your building, taking into account neighboring infrastructures and facilities.
- Secure dumpsters and other trash containers to prevent the hiding of explosives or other HAZMAT and to prevent unauthorized access to discarded papers and records.

In the event of an elevated or imminent threat:

- Increase monitoring, inspection, testing, and patrols of all utility services. Consider providing continuous security guard presence at critical utility points. Request assistance from local law enforcement, as necessary.
- Establish communication with utility service providers to review plans for responding to disruptions.

5. Special Considerations for Multi-use Districts & Adjacent Facilities

Recognize that security does not end at a building's perimeter. Considering adjacent facilities and the impact they have on a building is important. Commercial real estate is co-located with retail, malls, hotels, public assembly venues, airports, rail lines, transportation/subway terminals, and more. These adjacent facilities operate with their own distinct security needs, and as such, they require their own protective measures.

Buildings integrated with other facilities need to consider site and site-specific vulnerabilities applicable to both the building and the surrounding properties. In the interest of security, it is best to leave aside any tensions between neighbors or landlords/tenants.

When working with neighbors, consider the following general security measures:

- Consider what critical infrastructure, government, military, or recreational areas are in the local area that affect transportation, utilities, and collateral damage (e.g., how an attack at this facility would impact the building).
- Consider the type of businesses nearby and the impact they may have on daily or emergency operations. Factors to consider may include potential storage or use of hazardous materials, and type and number of visitors in the area.

- Partner with adjacent facilities and meet regularly to discuss common security issues, share information, and discuss local issues to assist in protecting your building. Meet regularly to discuss challenges.
- Communications is crucial in a multi-use district. Ensure that you are communication with area businesses to do the following:
  - Share threats
  - Discuss security measures
  - Conduct exercises
  - Discuss search and evacuation plans
  - Plan incident responses
- Consider developing a listserv for rapid communication.
- Involve local law enforcement and emergency responders.

6. Key Federal Protective Programs

Homeland Security Information Network (HSIN)

The Homeland Security Information Network (HSIN) is an Internet-based platform used by the U.S. Department of Homeland Security (DHS) to facilitate the sharing of information necessary for coordination, operational plans, mitigation, and response to incidents by the government and the private sector.

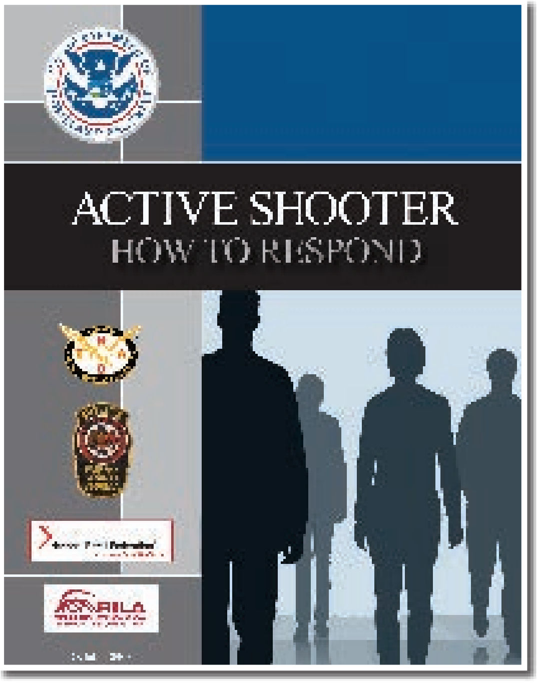
HSIN allows for secure, encrypted communications between DHS and the private sector, including sector-specific threat information. The Commercial Facilities Sector maintains an independent site on the HSIN portal.

Within the Commercial Facilities Sector portal, there is a specific portal for the Real Estate Subsector, allowing venue owners and operators to communicate with each other, independent from DHS or other Government agencies.

HSIN offers many dynamic resources and tools including:

- 24/7 availability
- Document Libraries, including:
  - *Active Shooter-How To Respond*
  - *Protective Measures Guide for U.S. Commercial Real Estate*
- Webinars
- Suspicious Activity Reporting Tool
- Secure Instant Messaging
- Web conferencing
- Incident reporting
- Common Operational Picture (COP), which provides situational awareness and analysis
- DHS OneView, which provides geographical visualization
- TRIPWire Community Gateway
- Announcements
- Discussion boards
- Task lists
- Calendars
- Really Simple Syndication (RSS) Feeds
- Online training materials

The HSIN network is open to security representatives, owners, and operators of commercial facilities. To gain access, send a request for membership to hsin.helpdesk@dhs.gov. Please include your name, official email address, phone number, organization, job title/ responsibilities, supervisor's name, supervisor's email address, phone number, and note that you are part of the Real Estate Subsector.



Requests received via email will be forwarded back to the Commercial Facilities Sector-Specific Agency for consideration.

DHS OneView

OneView is a secure, Web-based, geospatial visualization application (or "viewer") that allows for individual users to view and interact with data and application services within the DHS Geospatial Information Infrastructure (GII) and various external information from government and commercial sources.

OneView provides access to over 400 infrastructure data layers delivered as Web services via the GII, as well as population data and real-time situational awareness data for infrastructure impact analysis. Users may also add and use their own data for added context and utility. The foundational data set in OneView is provided by the Homeland Security

Infrastructure Program (HSIP), which includes data layers representing the 16 critical infrastructure sectors, national hazards, and base map layers.

OneView is currently available on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI).

TRIPwire Community Gateway

TRIPwire Community Gateway is a secure online portal designed specifically for the Nation's critical infrastructure owners, operators, and private security personnel. TRIPwire Community Gateway provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent IED incidents.

TRIPwire Community Gateway shares IED-related information tailored to each of the 16 critical infrastructure sectors as well as a Community Sector for educational institutions, in accordance with the National Infrastructure Protection Plan (NIPP). Sector partners benefit from increased communication, improved awareness of emerging threats, and access to resources and guidance on specific IED preventive and protective measures for their facilities and requirements. TRIPwire Community Gateway information is currently available on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) system.

Fusion Centers

Fusion Centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and State, local, tribal, territorial and private sector partners.

Located in States and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, and private sector security personnel to lawfully gather and share threat-related information. Fusion centers provide interdisciplinary expertise and situational awareness to inform decisionmaking at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

Fusion centers are owned and operated by State and local entities with support from Federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to Federal systems, technology, and grant funding. For additional information about fusion centers, see the National Network of Fusion Centers Fact Sheet.[30]

[30] U.S. Department of Homeland Security, National Network of Fusion Centers Fact Sheet, *http://www.dhs.gov/national-network-fusion-centers-fact-sheet*, (accessed June 28, 2013).

"If You See Something, Say Something"™

In July 2010, the Department of Homeland Security, at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something"™ public awareness campaign–a simple and effective program to raise public awareness of indicators of terrorism and violent crime and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-crime efforts.

A critical element of the DHS mission is ensuring that the civil rights and civil liberties of persons are not diminished by our security efforts, activities, and programs. Consequently, the "If You See Something, Say Something"™ campaign respects civil rights or civil liberties by emphasizing behavior, rather than appearance, in identifying suspicious activity.

Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and situations (e.g., an unattended backpack in a public place or someone trying to break into a restricted area) rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity. Only reports that document behavior reasonably indicative of criminal activity related to terrorism will be shared with Federal partners.

The "If You See Something, Say Something"™ campaign is being launched in conjunction with the rollout of the Nationwide Suspicious Activity Reporting Initiative (NSI).[31] The NSI is an administration-wide effort to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities. Led by the Department of Justice, the NSI is implemented in partnership with State and local officials across the Nation.

Both the "If You See Something, Say Something"™ campaign and the NSI underscore the concept that homeland security begins with hometown security, where an alert public plays a critical role in keeping our Nation safe.

Protective Security Advisors: Providing Community-Based Support

Established in 2004, the Protective Security Advisor (PSA) program[32] provides a DHS security expert as the link between State, local, tribal, and territorial organizations and DHS infrastructure protection resources. PSAs support DHS and our national protection mission by fostering improved coordination at the State and local level through their execution of training programs and by providing a local perspective to the national risk picture.

[31] Nationwide SAR Initiative http://nsi.ncirc.gov/documents/NSI_Overview.pdf, (accessed June 28, 2013).

[32] DHS Protective Security Advisors http://www.dhs.gov/protective-security-advisors, (accessed June 28, 2013).

With an average of 20 years of anti-terrorism and security experience, these dedicated critical infrastructure and vulnerability assessment experts are recruited from, live, and work in local communities. They provide a federally funded resource to communities and businesses to assist in the protection of critical assets.

The role of the PSA includes the following responsibilities:

- Supporting the development of the national risk picture by assisting in identifying, assessing, monitoring, and minimizing risk to critical assets at the State, local, or district level
- Facilitating, coordinating, and/or performing vulnerability assessments for local critical infrastructure
- Assisting (upon request) with security efforts coordinated by State Homeland Security Advisors
- Providing guidance on established security practices
- Conveying local concerns and sensitivities to the DHS and other Federal agencies
- Communicating requests for Federal protection training and exercises
- Providing reach-back capability to the DHS or other Federal Government resources
- Providing local context and expertise to DHS to ensure community resources are used appropriately, efficiently and effectively

For more information about the PSA program, contact: FOBAnalysts@hq.dhs.gov.

Vulnerability Assessments

The Department of Homeland Security conducts specialized facility assessments to identify vulnerabilities of critical infrastructure, including assets within the Commercial Facilities Sector and Real Estate Subsector. These vulnerability assessments provide the foundation of the risk-based implementation of protective programs designed to prevent, deter, and mitigate the risk of a terrorist attack while enabling timely, efficient response and restoration in an all-hazards post-event situation.

U.S. Department of Homeland Security's Business Continuity Planning Suite

The Business Continuity Planning (BCP) Suite was developed to assist businesses across all sectors with the need to create, improve, or update their business continuity plans. The Suite was designed to be user-friendly and scalable for optimal organizational use. It consists of three main components which include: BCP training, automated BCP and disaster recovery plan generators, and a self-directed exercise for testing an implemented BCP. Businesses can utilize this solution to maintain normal operations and exhibit resilience during a disruptive event.

For more information on the Business Continuity Planning Suite, contact: criticalmanufacturing@dhs.gov.

Active Shooter Preparedness

The Department of Homeland Security aims to enhance preparedness through a "whole community" approach by providing training, products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. In many cases, there is no pattern or method to the selection of victims by an active shooter, and these situations, by their very nature, are unpredictable and evolve quickly. DHS offers free courses, materials, and workshops to better prepare stakeholders to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.

To learn more about active shooter preparedness, visit http://www.dhs.gov/activeshooter

U.S. Department of Homeland Security's Cyber Security Evaluation Tool (CSET)

The Department of Homeland Security is responsible for protecting our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. The National Cyber Security Division coordinates the Department's efforts to secure cyberspace and our Nation's cyber assets and networks.

Critical infrastructures are dependent on information technology systems and computer networks for essential operations. Particular emphasis is placed on the reliability and resiliency of the systems that comprise and interconnect these infrastructures.

The Cyber Security Evaluation Tool (CSET) is a DHS product that assists organizations in protecting these key national cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.

To learn more about the CSET please contact: CSET@dhs.gov.

Joint Terrorism Task Forces

Joint Terrorism Task Forces (JTTFs) are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of Federal, State, and local law enforcement.

National Cybersecurity and Communications Integration Center (NCCIC)

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 center responsible for the production of a common operating picture for cyber and communications across Federal, State, and local government; intelligence and law enforcement communities; and the private sector. The NCCIC is operated within the Office of Cybersecurity and Communications, a component of the National Protection & Programs Directorate, (DHS). During a cyber or communications incident, the NCCIC serves as the national response center, able to bring the full capabilities of the Federal government to bear, in a coordinated manner, with State, local, and private sector partners. By integrating information from all partners – public and private, State and Federal, in both the cyber and communications arenas – the NCCIC creates and shares a common knowledge, coordinates response activities, and protects our Nation's critical networks.

To learn more about the NCCIC please contact: *NCCIC@DHS.gov*.

U.S. Department of Homeland Security's SAFETY ACT

The SAFETY Act provides important legal liability protections for providers of Qualified Anti-Terrorism Technologies - whether they are products or services. The goal of the SAFETY Act is to encourage the development and deployment of new and innovative anti-terrorism products and services by providing liability protections.

For more information on the SAFETY ACT, visit *https://www.safetyact.gov/*

List of Acronyms and Abbreviations

ACAMS	Automated Critical Asset Management System
BOMA	Building Owners and Managers Association International
CBR	Chemical, Biological, Radiological
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and High Yield Explosives
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control and Prevention
CSET	Cyber Security Evaluation Tool
DHS	Department of Homeland Security
EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
HAZMAT	Hazardous Material
H1N1	Swine Influenza
H5N1	Avian Influenza
HME	Home Made Explosive
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
HVAC	Heating, Ventilation, and Air Conditioning
HVE	Homegrown Violent Extremist

ID	Identification
IED	Improvised Explosive Device
IT	Information Technology
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
NDMS	National Disaster Medical System
NIPP	National Infrastructure Protection Plan
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
OPSEC	Operations Security
PPE	Personal Protective Equipment
RMS	Risk Management Series
SIP	Shelter-in-Place
SOP	Standard Operating Procedure
SSA	Sector-Specific Agency
VBIED	Vehicle-Borne Improvised Explosive Device
VIP	Very Important Person

Glossary of Key Terms

Accessible. Having the legally required features and/or qualities that ensure entrance, participation, and usability of places, programs, services, and activities by individuals with a wide variety of disabilities.[1]

Active Shooter. 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.[2]

Adversary. Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.[3]

Agency. A division of government with a specific function offering a particular kind of assistance.[4]

Aircraft Attack. A terrorist's use or control of an aircraft as a means to attack infrastructure targets directly.[5]

Asset. A person, structure, facility, information, material, or process that has value.[6]

Attack Method. Manner and means, including the weapon and delivery method, an adversary may use to cause harm to a target.[7]

Barriers. Used to define property boundaries and to enclose secured areas. Physical barriers include any objects that prevent access into a restricted area or through an entry portal, including fences, doors, turnstiles, gates, and walls. There are two categories of physical barriers: admission control and perimeter control.[8]

- Admission-control barriers are those used at entry points to selectively allow people to pass through. The most common admission-control barriers are swing doors, revolving doors, turnstiles, and portals. These may be operated mechanically or electronically in conjunction with electromagnetic door locks, keypads, or other entry-point screening mechanisms.
- Perimeter-control barriers establish a secure boundary around an area, and limit access to and from that area to admission control points. They can be constructed from a variety of materials, and may be designed to prevent some types of movement while permitting others (such as bollards that block motor vehicles while enabling pedestrians to pass through). Barriers can be placed to direct passenger flow and deter access to isolated or hidden locations.

[1] U.S. Department of Homeland Security, Federal Emergency Management Agency, Glossary of Terms, http://www.fema.gov/vii-glossary-terms, (accessed June 28, 2013)

[2] U.S. Department of Homeland Security, Active Shooter - How To Respond Desk Reference Guide, http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf, (accessed June 28, 2013).

[3] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[4] U.S. Department of Homeland Security, Federal Emergency Management Agency, Glossary of Terms, http://www.fema.gov/vii-glossary-terms, (accessed June 28, 2013).

[5] The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/PotentialTerroristAttackMethods.pdf, (accessed June 28, 2013).

[6] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[7] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[8] U.S. Department of Transportation, Transit Security Design Considerations, http://www.globalsecurity.org/security/library/report/2004/transit-security-design_appd.htm, (accessed June 28, 2013).

Biological Attack. A biological attack is the intentional release of a pathogen (disease causing agent) or biotoxin (poisonous substance produced by a living organism) against humans, plants, or animals. An attack against people could be used to cause illness, death, fear, societal disruption, and economic damage. An attack on agricultural plants and animals would primarily cause economic damage, loss of confidence in the food supply, and possible loss of life. It is useful to distinguish between two kinds of biological agents:

- Transmissible agents that spread from person to person (e.g., smallpox, Ebola) or animal to animal (e.g., foot and mouth disease).
- Agents that may cause adverse effects in exposed individuals but do not make those individuals contagious to others (e.g., anthrax, botulinum toxin).[9]

Bomb Threat. The communication through the use of mail, email, telephone, telegram, or other instrument of commerce; the willful making of any threat; or the malicious conveyance of false information knowing the same to be false which concerns an attempt being made, or to be made; to kill, injure, intimidate any individual; or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of an explosive.[10]

Capability. Means to accomplish a mission, function, or objective.[11]

Chemical Attack. The spreading of toxic chemicals with the intent to do harm. A wide variety of chemicals could be made, stolen, or otherwise acquired for use in an attack. Industrial chemical plants or the vehicles used to transport chemicals could also be sabotaged. Harmful chemicals that could be used in an attack include:

- Chemical weapons (warfare agents) developed for military use.
- Toxic industrial and commercial chemicals that are produced, transported, and stored in the making of petroleum, textiles, plastics, fertilizers, paper, foods, pesticides, household cleaners, and other products.
- Chemical toxins of biological origin such as ricin.[12]

Computer Virus. A program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then replicating itself. Some viruses are harmless, others may damage data files, and some may destroy files. Viruses can be spread through shared disks and other portable media. Email messages are currently the most common medium for spreading computer viruses.[13]

Commercial Facilities Sector. The Commercial Facilities Sector is comprised of a number of subsectors, including:

- Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers);
- Sports Leagues (e.g., professional sports leagues and federations);

[9] National Academies and the U.S. Department of Homeland Security, Biological Attack: Human Pathogens, Biotoxins, and Agricultural Threats, http://www.dhs.gov/xlibrary/assets/prep_biological_fact_sheet.pdf, (accessed June 28, 2013)

[10] University of Tennessee-Martin. Bomb Threat Information, http://www.utm.edu/alerts/bomb.php, (accessed June 28, 2013).

[11] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[12] National Academies and the U.S. Department of Homeland Security, Chemical Attack: Warfare Agents, Industrial Chemicals, and Toxins, http://www.dhs.gov/xlibrary/assets/prep_chemical_fact_sheet.pdf, (accessed June 28, 2013)

[13] U.S. Department of Homeland Security, Computer Emergency Readiness Team (US-CERT). Virus Basics, http://www.us-cert.gov/reading_room/virus.html, (accessed June 28, 2013)

- Gaming (e.g., casinos);
- Lodging (e.g., hotels, motels, conference centers);
- Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades);
- Entertainment and Media (e.g., motion picture studios, broadcast media);
- Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage); and
- Retail (e.g., retail centers and districts, shopping malls).

The diverse nature of assets within the Commercial Facilities Sector leads to a myriad of activities being performed. Facilities within this sector are generally not regulated at the Federal level and are designed for one of the following purposes: business activities (e.g., iconic office tower), personal commercial transactions (e.g., large regional mall), recreational pastimes (e.g., world famous amusement park), or accommodations (e.g., large iconic hotel or residential structure).[14]

The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Consequence. The effect of an event, incident, or occurrence.[15]

Countermeasure. An action, measure, or device that reduces an identified risk.[16]

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating effect on security, the national economy, public health or safety, or any combination thereof.[17]

Cyber Attack. A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.[18]

Cybersecurity Vulnerability Assessment (CSET). The CSET is a DHS product that assists organizations in protecting key national cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.[19]

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public

[14] U.S. Department of Homeland Security, Commercial Facilities Sector Training and Resources Web site, *http://www.dhs.gov/commercial-facilities-sector*, (accessed June 28, 2013).

[15] U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf*, (accessed June 28, 2013).

[16] U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf*, (accessed June 28, 2013).

[17] U.S. Department of Homeland Security, Critical Infrastructure Web site, *http://www.dhs.gov/what-critical-infrastructure*, (accessed June 28, 2013).

[18] U.S. Department of Defense, Cyberspace Glossary, *http://www.pcmag.com/encyclopedia_term/0,,t=&i=62535,00.asp*, (accessed June 28, 2013).

[19] U.S. Department of Homeland Security, Computer Emergency Readiness Team (US-CERT), Control Systems Security Program (CSSP), *http://www.us-cert.gov/control_systems/satool.html*, (accessed June 28, 2013).

safety answering points, and 911 communications systems and control systems.[20]

Deterrent. A measure that discourages an action or prevents an occurrence by instilling fear, doubt, or anxiety.[21]

Emergency. Any incident, whether natural or manmade, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the U.S. President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.[22]

Emergency Operations Center (EOC). The physical location in which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary workplace or may be located in a more central or permanently established workplace, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (i.e., fire, law enforcement, and medical services), by jurisdiction (i.e., Federal, State, regional, tribal, city, county), or some combination thereof.[23]

Emergency Operations Plan. An ongoing plan for responding to a wide variety of potential hazards.[24]

Evaluation. The process of examining, measuring, and/or judging how well an entity, procedure, or action has met or is meeting stated objectives.[25]

Function. A service, process, capability, or operation performed by an asset, system, network, or geographic area.[26]

Fusion Center. Many States and larger cities have created State and local fusion centers to share information and intelligence within their jurisdictions as well as with the Federal Government. The Department, through the Office of Intelligence and Analysis, provides personnel with operational and intelligence skills to the fusion centers.

This support is tailored to the unique needs of the locality and serves to:

- Help the classified and unclassified information flow,
- Provide expertise,
- Coordinate with local law enforcement and other agencies, and provide local awareness and access.[27]

Hazard. A natural or manmade source or cause of harm or difficulty.[28]

[20] U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, (accessed June 28, 2013).

[21] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[22] U.S. Department of Homeland Security, National Incident Management System, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, (accessed June 28, 2013).

[23] U.S. Department of Homeland Security, National Incident Management System, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, (accessed June 28, 2013).

[24] U.S. Department of Homeland Security, National Incident Management System, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, (accessed June 28, 2013).

[25] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[26] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[27] U.S. Department of Homeland Security. State and Local Fusion Centers, http://www.dhs.gov/state-and-major-urban-area-fusion-centers, (accessed June 28, 2013).

[28] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

Homegrown Violent Extremism (HVE): A national secure and trusted web-based portal for information sharing and collaboration between Federal, State, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.[29]

Homeland Security Information Network (HSIN). A national secure and trusted Web-based portal for information sharing and collaboration between Federal, State, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.[30]

Implementation. An act of putting a procedure or course of action into effect to support goals or achieve objectives.[31]

Improvised Explosive Device (IED). A homemade bomb and/or destructive device used to destroy, incapacitate, harass, or distract. IEDs are used by criminals, vandals, terrorists, suicide bombers, and insurgents.[32]

Incident. An occurrence, caused by either human action or natural phenomena, that may cause harm and require action.[33]

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.[34]

Intent. A state of mind or desire to achieve an objective.[35]

Interdependency. A mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.[36]

Local Government. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal entity, or in Alaska a Native Village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. See Section 2 (10), Homeland Security Act of 2002, P.L. 107–296, 116 Stat. 2135 (2002).[37]

[29] (U//FOUO) "Domestic Terrorism and Homegrown Violent Extremism Lexicon" (10 November 2011), U.S. Department of Homeland Security, Homeland Security Information Network – Intelligence, http://www.dhs.gov/hsin-intelligence, (accessed June 28, 2013)

[30] U.S. Department of Homeland Security, Homeland Security Information Network, http://www.dhs.gov/homeland-security-information-network, (accessed June 28, 2013).

[31] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[32] U.S. Department of Homeland Security, Improvised Explosive Device Fact Sheet, http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, (accessed June 28, 2013).

[33] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[34] U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, (accessed June 28, 2013).

[35] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[36] U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, (accessed June 28, 2013).

[37] U.S. Department of Homeland Security, National Incident Management System, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, (accessed June 28, 2013).

Lone Offender. An individual motivated by one or more violent extremist ideologies, who, operating alone, supports or engages in acts of violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor.[38]

Malicious Code. Any software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system.[39]

Maritime Attack. This attack method involves using a maritime vessel to undertake terrorist acts and activities within the maritime environment.[40]

Mitigation. The ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident.[41]

Natural Hazard. A source of harm or difficulty created by a meteorological, environmental, or geological phenomenon; or combination of phenomena.[42]

Network. A group of components that share information or interact with each other in order to perform a function (e.g., power plants, substations, and transmission lines constitute a network that creates and distributes electricity).[43]

Nuclear Attack. The use of a device that produces a nuclear explosion. A nuclear explosion is caused by an uncontrolled chain reaction that splits atomic nuclei (fission) to produce an intense wave of heat, light, air pressure, and radiation, followed by the production and release of radioactive particles.[44]

Physical Security. Describes measures used to protect assets (including computers) from damage caused by physical forces such as explosion, impact, and fire.[45]

Private Sector. Organizations and entities that are not part of any governmental structure. The private sector includes for profit and not-for-profit organizations, formal and informal structures, commerce and industry, private emergency response organizations, and private voluntary organizations.[46]

Protective Measures. Equipment, personnel, training, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures are designed to meet one or more of the following objectives:

Defend Respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack.

[38] (U//FOUO) "Domestic Terrorism and Homegrown Violent Extremism Lexicon" (10 November 2011), U.S. Department of Homeland Security, Homeland Security Information Network – Intelligence, http://www.dhs.gov/hsin-intelligence, (accessed June 28, 2013).

[39] National Security Agency, Guidance for Addressing Malicious Code, http://www.nsa.gov/ia/_files/Guidance_For_Addressing_Malicious_Code_Risk.pdf, (accessed June 28, 2013).

[40] The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/, (accessed June 28, 2013).

[41] U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, (accessed June 28, 2013).

[42] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[43] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[44] National Academies and the U.S. Department of Homeland Security, Nuclear Attack, http://www.dhs.gov/xlibrary/assets/prep_nuclear_fact_sheet.pdf, (accessed June 28, 2013).

[45] Congressional Research Service (CRS), Critical Infrastructure and Key Resources: Definition and Identification, http://www.fas.org/sgp/crs/RL32631.pdf, (accessed June 28, 2013).

[46] U.S. Department of Homeland Security, Federal Emergency Management Agency, Glossary of Terms, http://www.fema.gov/vii-glossary-terms, (accessed June 28, 2013).

Detect	Spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.
Deter	Make the facility more difficult to attack successfully.
Devalue	Lower the appeal of a facility to malicious actors; that is, make the facility less interesting as a target.

Radiological Attack. The spreading of radioactive material with the intent to do harm. Radioactive materials are used every day in laboratories, medical centers, food irradiation plants, and for industrial uses. If stolen or otherwise acquired, many of these materials could be used in a "radiological dispersal device" (RDD).[47]

Resilience. The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.[48]

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.[49]

Risk Assessment. A product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decisionmaking.[50]

Risk Management. A process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.[51]

Risk Mitigation. An application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.[52]

Scenario (Risk). A hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate.[53]

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The National Infrastructure Protection Plan (NIPP) addresses 16 Critical Infrastructure sectors.[54]

Security Awareness. The knowledge and attitude members of an organization possess regarding the protection of the physical and information assets of an organization.[55]

Spyware. Software that records the actions of a computer user without knowledge or consent. Some spyware can record user activities and keystrokes to capture passwords or other sensitive data as it is typed and send it to a remote

[47] National Academies and the U.S. Department of Homeland Security, Radiological Attack: Dirty Bombs and Other Devices, http://www.dhs.gov/xlibrary/assets/prep_radiological_fact_sheet.pdf, (accessed June 28, 2013).

[48] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[49] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[50] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[51] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[52] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[53] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[54] U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, (accessed June 28, 2013).

[55] Rutgers University, Security, Awareness, Training and Communication, http://rusecure.rutgers.edu/content/security-awareness-training-and-communication, (accessed June 28, 2013).

attacker. Some spyware can even allow the attacker to control the infected computer remotely.[56]

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.[57]

Target. An asset, network, system, or geographic area chosen by an adversary to be impacted by an attack.[58]

Terrorism. As defined under the Homeland Security Act of 2002, any activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources; is a violation of the criminal laws of the United States or of any State or other subdivision of the United States in which it occurs; and is intended to intimidate or coerce the civilian population or influence or affect the conduct of a government by mass destruction, assassination, or kidnapping. See Section 2 (15), Homeland Security Act of 2002, P.L. 107–296, 116 Stat. 2135 (2002).

Threat. A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.[59]

Threat Assessment. A process of identifying or evaluating entities, actions, or occurrences, whether natural or manmade, that have or indicate the potential to harm life, information, operations, and/or property.[60]

Trojan Horse. A computer program that hides a virus or other potentially damaging program. A Trojan horse can be a program that purports to do one action when, in fact, it is performing a malicious action on your computer. Trojan horses can be included in software that you download for free or as attachments in email messages.[61]

Vehicle-borne Improvised Explosive Device (VBIED). A device that integrates a vehicle and an explosive device specifically for detonation against a target.[62]

Vulnerability. A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.[63]

Vulnerability Assessments. A product or process for identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards.[64]

Worms. A type of virus that can spread without human interaction. Worms often spread from computer to computer and take up valuable memory and network bandwidth, which can cause a computer

[56] U.S. Department of Homeland Security, Computer Emergency Readiness Team (US-CERT), Spyware, http://www.us-cert.gov/reading_room/spywarehome_0905.pdf, (accessed June 28, 2013).

[57] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[58] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[59] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[60] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[61] U.S. Department of Homeland Security, Computer Emergency Readiness Team (US-CERT), Virus Basics, http://www.us-cert.gov/reading_room/virus.html, (accessed June 28, 2013)

[62] The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/, (accessed June 28, 2013).

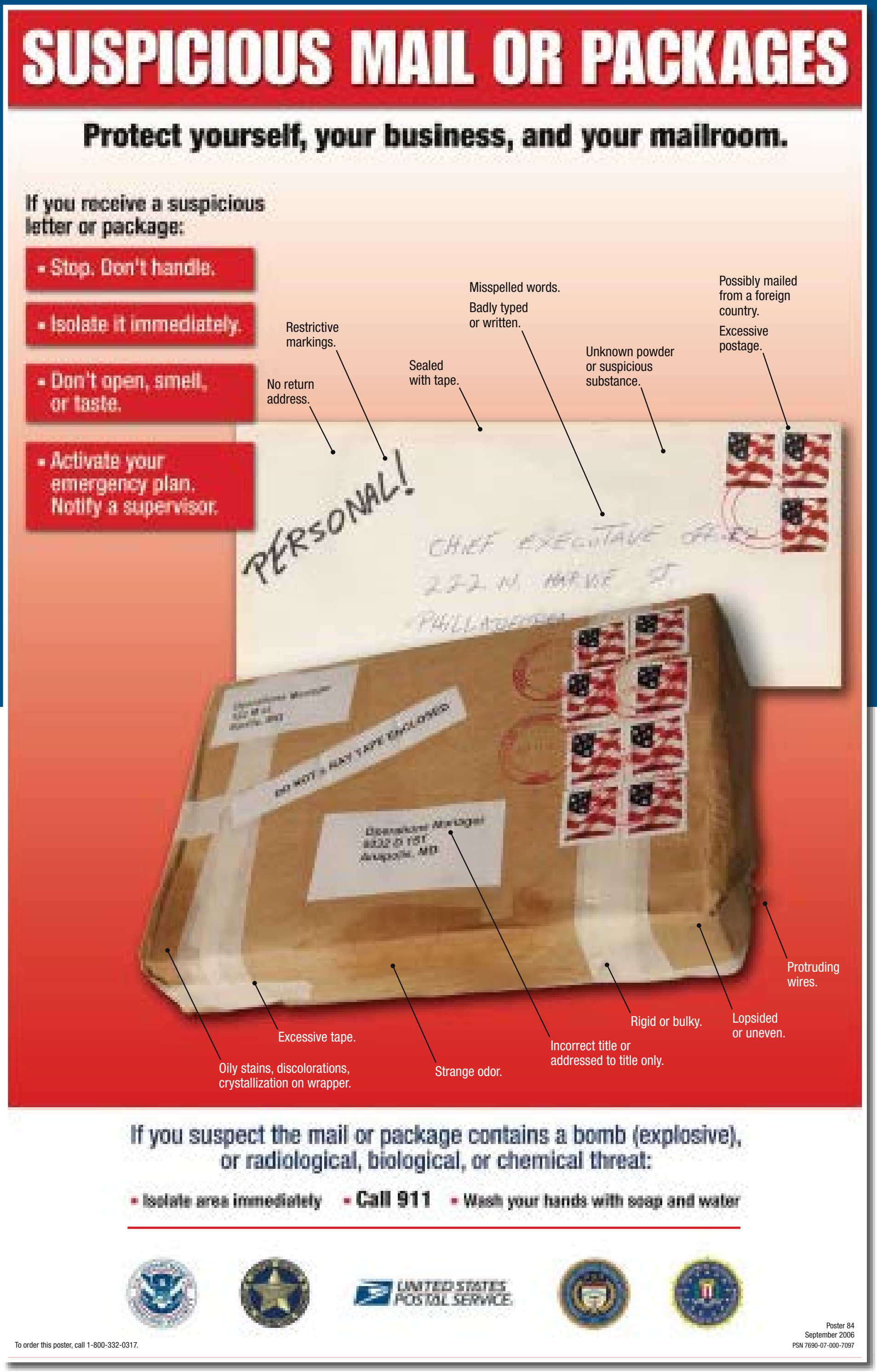
[63] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

[64] U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf, (accessed June 28, 2013).

to stop responding. Worms can also allow attackers to gain access to your computer remotely.[65]

[65] U.S. Department of Homeland Security, Computer Emergency Readiness Team (US-CERT), Virus Basics, *http://www.us-cert.gov/reading_room/virus.html*, (accessed June 28, 2013).

Appendix A: Suspicious Mail or Packages


PERSONAL!
CHIEF EXECUTIVE OFFICER
222 N HARVIE ST
PHILADELPHIA
DO NOT X-RAY TAPE ENCLOSED

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom.

If you receive a suspicious letter or package:

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.

Restrictive markings.

No return address.

Sealed with tape.

Misspelled words.

Badly typed or written.

Unknown powder or suspicious substance.

Possibly mailed from a foreign country.

Excessive postage.

Protruding wires.

Lopsided or uneven.

Rigid or bulky.

Incorrect title or addressed to title only.

Strange odor.

Excessive tape.

Oily stains, discolorations, crystallization on wrapper.

If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

UNITED STATES POSTAL SERVICE

To order this poster, call 1-800-332-0317.

Poster 84
September 2006
PSN 7690-07-000-7097

USPS Suspicious Mail or Packages Poster:
http://about.usps.com/posters/pos84.pdf

Terrorists may attempt to send chemical, biological, or radiological (CBR) materials through the mail. Although it is not possible to list all CBR indicators because of the diversity of the materials, a sample list is provided below.

Suspicious mail may have one or more of the following characteristics:

- An unfamiliar sender
- No return address
- Inaccurate address, possibly to someone no longer employed with the venue
- Writing in an unfamiliar style
- Unusual postmarks, or a substantial overpayment of postage
- A padded envelope
- Unusually heavy for its size
- Marked as "personal" or "confidential"
- Oddly shaped or lopsided
- Pin-sized hole(s) visible in the envelope
- A strange smell
- Stained or damp packaging

Indicators of chemical, biological or radiological materials in the mail include:

- Finely powdered material, possibly with the consistency of sugar
- Sticky substances
- Sprays and vapors
- Metal or plastic pieces
- Strange smell (although some CBR materials are odorless and tasteless)

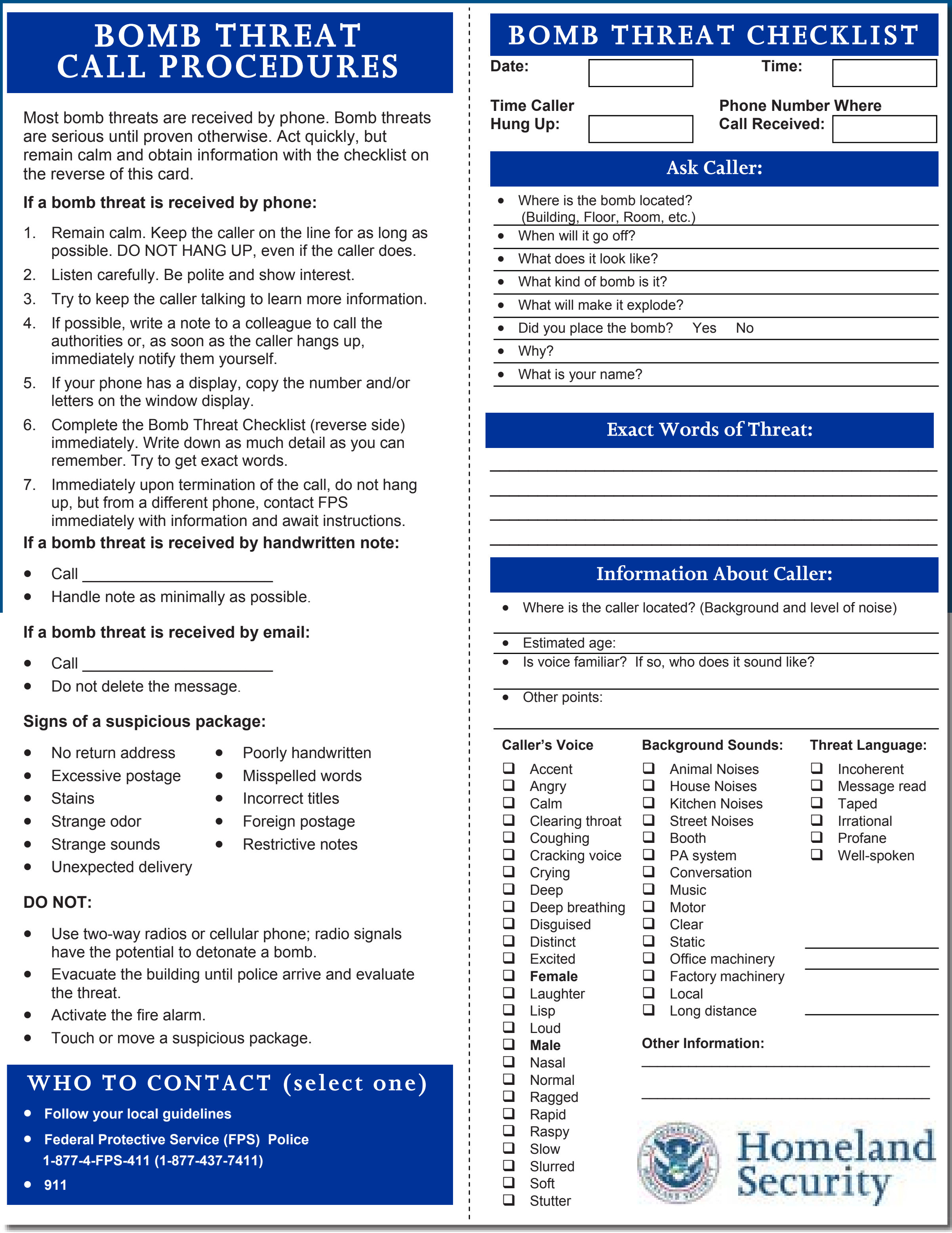
If you receive a suspicious letter or package:

- Stop
- Do not handle it
- Isolate it immediately
- Do not open, smell, or taste it
- Notify a supervisor
- Activate your emergency operations plan

If you suspect the mail or package contains a bomb (explosive), radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

Appendix B: Bomb Threat Checklist



BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (reverse side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call ______________________
- Handle note as minimally as possible.

If a bomb threat is received by email:

- Call ______________________
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- **Follow your local guidelines**
- **Federal Protective Service (FPS) Police**
  1-877-4-FPS-411 (1-877-437-7411)
- **911**

BOMB THREAT CHECKLIST

Date: ______ **Time:** ______

Time Caller Hung Up: ______ **Phone Number Where Call Received:** ______

Ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.) ______
- When will it go off? ______
- What does it look like? ______
- What kind of bomb is it? ______
- What will make it explode? ______
- Did you place the bomb? Yes No ______
- Why? ______
- What is your name? ______

Exact Words of Threat:

____

____

____

____

Information About Caller:

- Where is the caller located? (Background and level of noise) ______
- Estimated age: ______
- Is voice familiar? If so, who does it sound like? ______
- Other points: ______

Caller's Voice

❑ Accent
❑ Angry
❑ Calm
❑ Clearing throat
❑ Coughing
❑ Cracking voice
❑ Crying
❑ Deep
❑ Deep breathing
❑ Disguised
❑ Distinct
❑ Excited
❑ **Female**
❑ Laughter
❑ Lisp
❑ Loud
❑ **Male**
❑ Nasal
❑ Normal
❑ Ragged
❑ Rapid
❑ Raspy
❑ Slow
❑ Slurred
❑ Soft
❑ Stutter

Background Sounds:

❑ Animal Noises
❑ House Noises
❑ Kitchen Noises
❑ Street Noises
❑ Booth
❑ PA system
❑ Conversation
❑ Music
❑ Motor
❑ Clear
❑ Static
❑ Office machinery
❑ Factory machinery
❑ Local
❑ Long distance

Threat Language:

❑ Incoherent
❑ Message read
❑ Taped
❑ Irrational
❑ Profane
❑ Well-spoken

____

____

____

Other Information:

____

____

Homeland Security

DHS Bomb Threat Call Procedures Checklist:
http://emilms.fema.gov/is906/assets/ocso-bomb_threat_samepage-brochure.pdf

Appendix C: Additional Resources–Web Sites

U.S. Department of Homeland Security's Commercial Facilities Sector Training and Resources Web Site

Protecting and ensuring the continuity of the critical infrastructure of the United States are essential to our Nation's security, public health and safety, economic vitality, and way of life. The following resources are available for download at the DHS Commercial Facilities Sector Training and Resources Web site:

- *Active Shooter – How To Respond*. A desk reference guide; a reference poster; and a pocket-size reference card to address how employees, managers, training staff, and human resources personnel can mitigate the risk of and appropriately react in the event of an active shooter situation.
- *Check It!* This video is designed to raise the level of awareness for front line facility employees by highlighting the indicators of suspicious activity. It also provides information to help employees properly search bags in order to protect venues and patrons.
- *What's in Store: Ordinary People/Extraordinary Events*. Designed to raise the level of awareness for retail and shopping center employees by highlighting the indicators of suspicious activity, this video provides information to help employees identify and report suspicious activities and threats in a timely manner.

These resources and more can be found in the Commercial Facilities Sector-Specific Training and Resources section at: *http://www.dhs.gov/cfsector*.

U.S. Department of Homeland Security's Automated Critical Asset Management System (ACAMS)

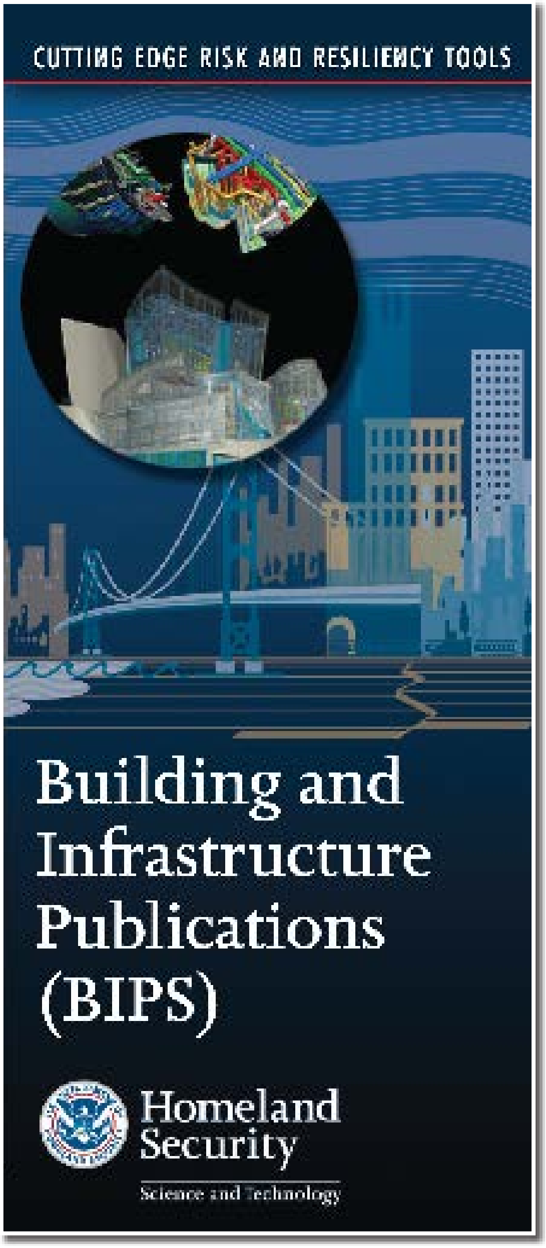
The Automated Critical Asset Management System (ACAMS) is a Web-enabled information services portal that helps State, local, tribal, and territorial governments build critical infrastructure protection programs. ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel:

- Collect and use critical infrastructure asset data,
- Assess critical infrastructure asset vulnerabilities,
- Develop all-hazards incident response and recovery plans, and
- Build public-private partnerships.

For questions, email *ACAMShelp@hq.dhs.gov*.

U.S. Department of Homeland Security's Building and Infrastructure Protection Series (BIPS)

The Building and Infrastructure Protection Series (BIPS) is a series of publications and software tools developed by the U.S. Department of Homeland Security Science & Technology Directorate (S&T) to provide guidance on risk assessment and mitigation against multi-hazard events. The series emphasizes strengthening and protecting critical infrastructure from the impacts of a terrorist attack. The objectives of the publications and software tools are to reduce physical damage to structural and nonstructural components of buildings and critical infrastructure, and to reduce resultant casualties from impact events that include:


CUTTING EDGE RISK AND RESILIENCY TOOLS
Building and Infrastructure Publications (BIPS)
Homeland Security
Science and Technology

- Manmade hazards, including explosive blast; chemical, biological, and radiological (CBR) agents; and
- Natural hazards, including floods, hurricanes, earthquakes, and other natural disaster events.

http://www.dhs.gov/building-and-infrastructure-protection-series-tools-0

BIPS 04: Integrated Rapid Visual Screening (IRVS) of Buildings

This tool is designed to quantify the risk and resilience of a single building or a group of buildings to manmade and selected natural hazards capable of causing catastrophic losses in fatalities, injuries, damages, or business interruption. The IRVS of Buildings covers 15 building types and addresses 20 hazardous events: blast (external/internal); intrusions; external chemical, biological, and radiological releases (from 100, 300, and 1,000 feet); earthquakes (ground shaking and ground failure); floods (still water and velocity surge); wind (hurricane, tornado, and other wind events); landslide (from rainfall and earthquakes); and fire (from earthquakes, blast, or arson). IRVS-ISC provides a low cost, rapid method of assessing Federal buildings based on the Interagency Security Committee criteria. In addition, the IRVS Cloud, currently in development, will assess climate change (including floods, severe weather events, sea level rise, and temperature change) and undesirable natural hazard events (including earthquakes, drought, and wildfire) based on geographic region. http://www.dhs.gov/bips-04-integrated-rapid-visual-screening-series-irvs-buildings.

BIPS 06/FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings

This manual is a revised and expanded version of FEMA 426. BIPS 06 provides an updated version of risk assessment techniques, a new concept on infrastructure resiliency, and identifies new protective measures and emerging technologies to protect the built environment. The objective of this manual is to reduce physical damage to structural and non-structural components of buildings and related infrastructure; and also to reduce resultant casualties during conventional bomb attacks; as well as attacks using chemical, biological, and radiological agents. http://www.dhs.gov/bips-06fema-426-reference-manual-mitigate-potential-terrorist-attacks-against-buildings-2nd-edition

FEMA 452: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings

This how-to-guide outlines methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. The methods presented provide a means to assess risks and to make decisions about how to mitigate them. The scope of the methods includes reducing physical damage to structural and non-structural components of buildings and related infrastructure; and reducing resultant casualties during conventional bomb attacks; as well as attacks involving chemical, biological, and radiological (CBR) agents. http://www.fema.gov/media-library/assets/documents/4608?id=1938

U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT)

The Computer Emergency Readiness Team (US-CERT) is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT collaborates with Federal agencies, the private sector, the research community, State and local governments, and international entities. By analyzing incidents reported by these entities and coordinating with national security incident response centers responding to incidents on both classified and unclassified systems, US-CERT disseminates reasoned and actionable cybersecurity information to the public. http://www.us-cert.gov/cas/signup.html

US-CERT encourages reporting any suspicious activity, including cybersecurity incidents, possible malicious code, vulnerabilities, and phishing related scams. http://www.us-cert.gov

U.S. Department of Homeland Security's Protect Your Workplace Campaign

The Department of Homeland Security posters provide guidance on physical and cybersecurity; and how to report suspicious behavior, activity, and cyber incidents. Posters are available for download at http://www.us-cert.gov/reading_room/distributable.html.

U.S. Department of Homeland Security's Ready.gov

Ready.gov's section for businesses, Ready Business, outlines common-sense measures business owners and managers can take to start getting ready. It provides practical steps and easy-to-use templates to help companies plan for their future, as well as useful links to resources providing more detailed business continuity and disaster preparedness information. http://www.ready.gov/business

U.S. Department of Homeland Security's Stop. Think. Connect

The Stop. Think. Connect. Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. To learn more about the campaign, please visit http://www.dhs.gov/files/events/stop-think-connect.shtm.

All Hazards Consortium

The All Hazards Consortium (AHC) is a State-sanctioned, 501c3 non-profit organization focused on homeland security, emergency management, and business continuity issues in the Mid-Atlantic and Northeast regions of the United States. Serving State/local governments and the infrastructure owners and operators in the private sector, the AHC provides an "enabling framework" which allows various stakeholders to come together on specific projects and issues, sometimes with competing or overlapping interests, to collaborate on common initiatives that result in unique benefits to each group. *http://www.ahcusa.org/*

American Red Cross

As part of a worldwide movement that offers neutral humanitarian care to the victims of war, the American Red Cross distinguishes itself by also aiding victims of devastating natural disasters. Over the years, the organization has expanded its services, always with the aim of preventing and relieving suffering. *http://www.redcross.org*.

American Association of Poison Control Centers (AAPCC)

The American Association of Poison Control Centers (AAPCC) provides a network of toxicology experts ready to speak on more than 20 subject area specialties, including chemical and biological weapons, "pharming" (the misuse of prescription drugs), carbon monoxide, and childhood poisoning. AAPCC member poison centers maintain a 24/7 Poison Help hotline. The Poison Help hotline provides immediate access to poison-exposure management instructions and information on potential poisons. *http://www.aapcc.org/DNN/*

U.S. Army Chemical, Biological, Radiological, Nuclear (CBRN) School

The Chemical, Biological, Radiological, Nuclear (CBRN) School trains Joint and International Service members, develops leaders, supports training in units, develops multiservice and Army doctrine, builds the future CBRN force, and is the Joint Combat Developer for the Joint Chemical, Biological, Radiological, and Nuclear Defense Program. *http://www.wood.army.mil/newweb/chemical/*

U.S. Army Technical Escort Unit

The 20th Support Command integrates, coordinates, deploys, and provides trained and ready Chemical, Biological, Radiological, Nuclear, and High Yield Explosives (CBRNE) forces. The unit is capable of exercising command and control of specialized CBRNE operations to support Joint and Army force commanders primarily for overseas contingencies and warfighting operations, but also in support of homeland defense. The unit maintains technical links with appropriate Joint, Army, Federal and State CBRNE assets, as well as the research, development, and technical communities to assure Army CBRNE response readiness. *http://www.cbrne.army.mil/*

ASIS International

ASIS International is the preeminent organization for security professionals, dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, as well as specific security topics. *http://www.asisonline.org/*

ASIS International High-Rise Security and Fire Life Safety, 3rd Ed

This book is a comprehensive reference for managing security and fire life safety operations within high-rise buildings. It spells out the unique characteristics of skyscrapers from a security and fire life safety perspective, details the type of security and life safety systems commonly found in them, outlines how to conduct risk assessments, and explains security policies and procedures designed to protect life and property. https://www.asisonline.org/ASIS-Store/Products/Pages/High-Rise-Security-and-Fire-Life-Safety-3rd-Ed.aspx

ASIS International Pre-Employment Background Screening Guideline

This guideline presents practical information concerning the value of pre-employment background screening, the importance of the application form, important legal issues and considerations (such as the Fair Credit Reporting Act, privacy issues, State laws, rules, and regulations), the key elements of pre-employment background screening, the types of information to utilize in verifying the key elements, the use of credit card reporting agencies in pre-employment background screening, and an appendix of a sample pre-employment background screening flow chart. The guideline is available as a single, free download to ASIS members and is available for purchase to non-members. http://www.asisonline.org/guidelines/published.htm.

ASIS International Security and Life Safety for the Commercial High-Rise

The risk assessment guidelines presented in this book are oriented toward protection of a site's personnel and physical assets. Guidelines would also generally apply to protection of computer data, hardware, and software. The security guidance discussed in this book will assist individual companies to assess their properties and determine how best to protect their assets. https://www.asisonline.org/ASIS-Store/Products/Pages/Security-and-Life-Safety-for-the-Commercial-High-Rise.aspx

Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors

This guide, produced by the Department of Homeland Security and the Interagency Security Committee, is designed to provide mail center managers, their supervisors, and an organization's security personnel with a framework for understanding and mitigating risks posed to an organization by the mail and packages it receives and delivers on a daily basis. The best practices guide outlines the most efficient and effective processes and procedures to handle and screen mail entering facilities for chemical, biological, radiological, nuclear, and explosive (CBRNE) threats. It includes a discussion of alternative technologies that can be employed and a recommendation for the proper location and construction of a mail screening facility. https://cs.hsin.gov/gf-sites/iscdocs/fouodocs/default.aspx

Building Owners and Managers Association (BOMA) International

The Building Owners and Managers Association (BOMA) International is an international federation of more than 100 local associations and affiliated organizations. Founded in 1907, its 16,500-plus members own or manage more than nine billion square feet of commercial properties. BOMA International's mission is to enhance the human, intellectual and physical assets of the commercial real estate industry through advocacy, education, research, standards, and information. http://www.boma.org

Building Owners and Managers Association (BOMA) International's Emergency Preparedness Guidebook

This BOMA guidebook is the industry's most up-to-date guide to help property professionals prepare for and respond to a broad range of potential threats. The guidebook walks the user step-by-step through the four phases of emergency management: 1) Mitigation, 2) Preparedness, 3) Response, and 4) Recovery; to help ensure tenant safety and building security during emergency situations. Several types of emergencies are covered: accidents such as fires, public health emergencies, elevator outages, and airplane collisions; earth and weather events such as floods, earthquakes, hurricanes and tornadoes; and criminal and terror acts such as terrorism, bombs, active shooter, and workplace violence. There is also an in-depth chapter on building an effective communications plan and checklists throughout to help users organize every step of their preparedness plan. http://store.boma.org/products/emergency-preparedness-guidebook

Centers for Disease Control and Prevention (CDC)

The Centers for Disease Control and Prevention (CDC) serves as the national focus for developing and applying disease prevention and control, environmental health, health promotion, and health education activities designed to improve the health of the people of the United States. CDC.gov provides users with credible, reliable health information, and serves as CDC's primary online communication channel. http://www.cdc.gov/

Centers for Disease Control and Prevention's Bioterrorism Preparedness and Response

This site is intended to increase the Nation's ability to prepare for and respond to public health emergencies. http://www.bt.cdc.gov/

Community Emergency Response Teams (CERT)

The CERT Program educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Using the training learned in the classroom and during exercises, CERT members can assist others in their neighborhood or workplace following an event when professional responders are not immediately available to help. http://www.citizencorps.gov/cert/

U.S. Environmental Protection Agency (EPA) Emergency Management

To ensure the Nation is better prepared for environmental emergencies, the Environmental Protection Agency (EPA) is working with other Federal partners to prevent accidents and maintain superior response capabilities. One of EPA's roles is to provide information about response efforts, regulations, tools, and research that will help the regulated community, government entities, and concerned citizens prevent, prepare for, and respond to emergencies. http://www.epa.gov/emergencies/index.htm

E-Verify

The U.S. Department of Homeland Security is working to stop unauthorized employment. By using E-Verify to determine the employment eligibility of their employees, companies become part of the solution in addressing this problem. E-Verify is an Internet-based system that compares information from an employee's Form I-9, *Employment Eligibility Verification*, to data from the U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility. http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=75bce2e261405110VgnVCM1000004718190aRCRD&vgnextchannel=75bce2e261405110VgnVCM1000004718190aRCRD

U.S. Food & Drug Administration (FDA) – ALERT Initiative

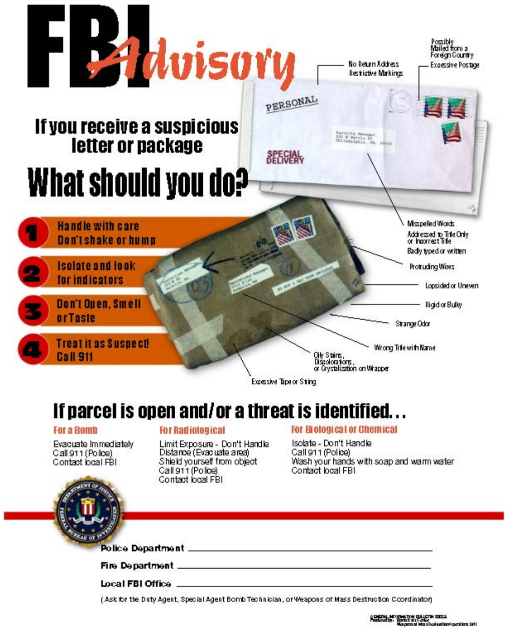
The ALERT initiative is intended to raise the awareness of State and local government agency and industry representatives regarding food defense issues and preparedness. It is generic enough to apply to all aspects of the farm-to-table supply chain and is designed to spark thought and discussion with a variety of stakeholders. ALERT identifies five key points that industry and businesses can use to decrease the risk of intentional food contamination at their facility. http://www.fda.gov/Food/FoodDefense/ToolsEducationalMaterials/ucm353774.htm

U.S. Food & Drug Administration (FDA) – Employees FIRST

Employees FIRST is a Food and Drug Administration initiative that food industry managers can include in their ongoing employee food defense training programs. Employees FIRST educates front-line food industry workers from farm-to-table about the risk of intentional food contamination and the actions they can take to identify and reduce these risks. http://www.fda.gov/Food/FoodDefense/ToolsEducationalMaterials/ucm295997.htm

Federal Bureau of Investigation (FBI)

The printable FBI Advisory outlines the basic identification of a suspicious package and the actions that should be taken if personnel encounter such a package. http://www.adl.org/security/fbi.pdf



FBI Advisory

If you receive a suspicious letter or package

What should you do?

1 Handle with care
Don't shake or bump

2 Isolate and look for indicators

3 Don't Open, Smell or Taste

4 Treat it as Suspect!
Call 911

Possibly Mailed from a Foreign Country
Excessive Postage
No Return Address
Restrictive Markings
PERSONAL
SPECIAL DELIVERY
Misspelled Words
Addressed to Title Only or Incorrect Title
Badly typed or written
Protruding Wires
Lopsided or Uneven
Rigid or Bulky
Strange Odor
Wrong Title with Name
Oily Stains, Discolorations, or Crystalization on Wrapper
Excessive Tape or String

If parcel is open and/or a threat is identified...

For a Bomb
Evacuate Immediately
Call 911 (Police)
Contact local FBI

For Radiological
Limit Exposure - Don't Handle
Distance (Evacuate area)
Shield yourself from object
Call 911 (Police)
Contact local FBI

For Biological or Chemical
Isolate - Don't Handle
Call 911 (Police)
Wash your hands with soap and warm water
Contact local FBI

Police Department ______________________

Fire Department ______________________

Local FBI Office ______________________

(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)

GENERAL INFORMATION BULLETIN [illegible]
Produced by: Bomb Data Center
Weapons of Mass Destruction Operations Unit

Federal Emergency Management Agency (FEMA)

FEMA's mission is to support citizens and first responders to ensure that as a nation we work together to build, sustain and improve our capability to prepare for, protect against, respond to, recover from and mitigate all hazards. http://www.fema.gov/

FEMA – Comprehensive Preparedness Guide 301: Interim Emergency Planning Guide for Special Needs Populations

This guide is intended as a tool for State, territorial, tribal, and local emergency managers in the development of emergency operations plans that are inclusive of the entire population of a jurisdiction of any size. It provides recommendations for planning for special needs populations. http://serve.mt.gov/wp-content/uploads/2010/10/CPG-301.pdf

FEMA Independent Study Program

The Emergency Management Institute (EMI) offers self-paced courses designed for people who have emergency management responsibilities and the general public. All are offered free-of-charge to those who qualify for enrollment. FEMA's Independent Study Program offers courses that support the nine mission areas identified by the *National Preparedness Goal: Incident Management, Operational Planning, Disaster Logistics, Emergency Communications, Service to Disaster Victims, Continuity Programs, Public Disaster Communications, Integrated Preparedness, and Hazard Mitigation.* http://training.fema.gov/IS/

Four recent critical infrastructure cross-sector training courses available online through EMI include:

- *Workplace Security Awareness* (IS-906). This training course provides guidance to individuals and organizations on how to improve the security in your workplace. http://training.fema.gov/EMIWeb/IS/is906.asp
- *Active Shooter – What You Can Do* (IS-907). This training course provides the public with guidance on how to prepare for and respond to active shooter crisis situations. The course was developed by the Office of Infrastructure Protection through a collaborative process that included representatives from the Commercial Facilities Sector and FEMA EMI. Development also included consultation with the Federal Law Enforcement Training Center. http://training.fema.gov/EMIWeb/IS/IS907.asp
- *Surveillance Awareness: What You Can Do* (IS-914). This training course makes critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance. https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-914
- *Protecting Critical Infrastructure Against Insider Threats* (IS-915). This training course provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure. https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-915

FEMA Security Risk Management Series (RMS) Publications

The Risk Management Series (RMS) is a FEMA series intended to provide design guidance for mitigating multi-hazard events. The series includes a large cadre of manmade disaster publications intended to strengthen the building inventory to reduce the potential impact from the forces that might be anticipated in a terrorist assault. The objective of the series is to reduce physical damage to structural and nonstructural components of buildings and related infrastructure, and to reduce resultant casualties from impact by conventional bombs, CBR agents, earthquakes, floods, and high winds. The intended audience includes architects and engineers working for private institutions, building owners/operators/managers, and State and local government officials working in the building sciences community. http://www.fema.gov/mitigation/security-risk-management-series-publications

Publications in this series of particular interest to the Commercial Real Estate industry include, but are not limited to:

- FEMA 430: *Site and Urban Design for Security: Guidance against Potential Terrorist Attacks* http://www.fema.gov/media-library/assets/documents/12746?id=3135
- FEMA 452: *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks*

http://www.fema.gov/plan/prevent/rms/rmsp452.shtm

- FEMA 453: *Safe Rooms and Shelters -- Protecting People Against Terrorist Attacks* http://www.fema.gov/media-library/assets/documents/4498?id=1910
- FEMA 455: *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks* http://www.fema.gov/media-library/assets/documents/2298?id=1567
- FEMA 459: *Incremental Protection for Existing Commercial Buildings from Terrorist Attacks* https://www.fema.gov/media-library/assets/documents/13311?id=3270

FEMA – Rapid Visual Screening of Buildings for Potential Seismic Hazards: A Handbook. Second Edition

This handbook presents a method to quickly identify, inventory, and rank buildings posing risk of death, injury, or severe curtailment in use following an earthquake. The Rapid Visual Screening procedure can be used by trained personnel to identify potentially hazardous buildings with a 15 to 30-minute exterior inspection, using a data collection form included in the handbook. http://www.fema.gov/media-library/assets/documents/15212?id=3556

Flu.gov

A Federal Government Web site managed by the U.S. Department of Health & Human Services, Flu.gov provides comprehensive government-wide information on seasonal, H1N1 (swine), H5N1 (avian/bird), H3N3, and pandemic flu information for the general public, health, and emergency preparedness professionals, policy makers, government and business leaders, school systems, and local communities. http://www.flu.gov/

U.S. Department of Health and Human Services' (HHS) National Disaster Medical System

The National Disaster Medical System (NDMS) is a federally coordinated system that augments the Nation's medical response capability. The overall purpose of the NDMS is to supplement an integrated national medical response capability for assisting State and local authorities in responding to the medical impacts of major peacetime disasters and to provide support to the military and the Department of Veterans Affairs medical systems in caring for casualties evacuated to the United States from overseas conventional armed conflicts. http://www.hhs.gov/aspr/opeo/ndms/

InfraGard

InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard chapters are geographically linked with FBI Field Office territories. http://www.infragard.net/

National Emergency Management Association (NEMA)

The National Emergency Management Association (NEMA) is the professional association of and for emergency management directors from all 50 states, eight territories, and the District of Columbia. NEMA provides national leadership and expertise in comprehensive emergency management; serves as a vital emergency management information and assistance resource; and advances continuous improvement in emergency management through strategic partnerships, innovative programs, and collaborative policy positions. http://www.nemaweb.org/

National Fire Protection Association (NFPA)

The National Fire Protection Association (NFPA) is the world's leading advocate of fire prevention and an authoritative source on public safety. NFPA develops, publishes, and disseminates more than 300 consensus codes and standards intended to minimize the possibility and effects of fire and other risks. http://www.nfpa.org

National Fire Prevention Association – NFPA 730: Guide for Premises Security

The uniform guidelines in NFPA 730: *Guide for Premises Security* helps accurately assess vulnerability and design appropriate security plans for all occupancy types, from one- and two-family dwellings to large industrial complexes. Provisions describe construction, protection, and occupancy features and practices intended to reduce security risks. The guide also covers protocols for special events and the roles and responsibilities of security personnel. http://www.nfpa.org/catalog/product.asp?title=Code-730-2008-Premises-Security&pid=73008&src=nfpa&order_src=A292

National Weather Service (NOAA)

The National Weather Service (NWS) which is part of the National Oceanic and Atmospheric Administration (NOAA) provides weather, water, and climate data, forecasts and warnings for the protection of life and property and enhancement of the national economy. Many of their products are broadcast on NOAA Weather Radio, a network of radio transmitters that broadcasts weather forecasts, severe weather statements, watches, and warnings 24 hours a day. http://www.weather.gov/

New York City Police Department's (NYPD) – Engineering Security: Protective Design for High Risk Buildings

The New York City Police Department developed a guide entitled *Engineering Security: Protective Design for High Risk Buildings* to aid the New York City building community by providing information on how to prevent and mitigate the effects of a terrorist attack on a building. This guide focuses on buildings: how to identify the very limited number of structures that present especially great terrorist risks, and how to build or retrofit them in ways that mitigate those risks. http://www.nyc.gov/html/nypd/html/counterterrorism/engineeringsecurity.shtml

U.S. Occupational Safety & Health Administration (OSHA)

The Occupational Safety and Health Administration's mission is to prevent work-related injuries, illnesses, and deaths by issuing and enforcing rules (called standards) for workplace safety and health. http://www.osha.gov

Overseas Advisory Council (OSAC)

The Overseas Advisory Council (OSAC) is a Federal Advisory Committee with a U.S. Government charter to promote security cooperation between American business and private sector interests worldwide and the U.S. Department of State. OSAC is currently comprised of a 34-member core Council, an Executive Office, more than 135 Country Councils, and more than 4,500 constituent member organizations. http://www.osac.gov/

Real Estate Information Sharing & Analysis Center (ISAC)

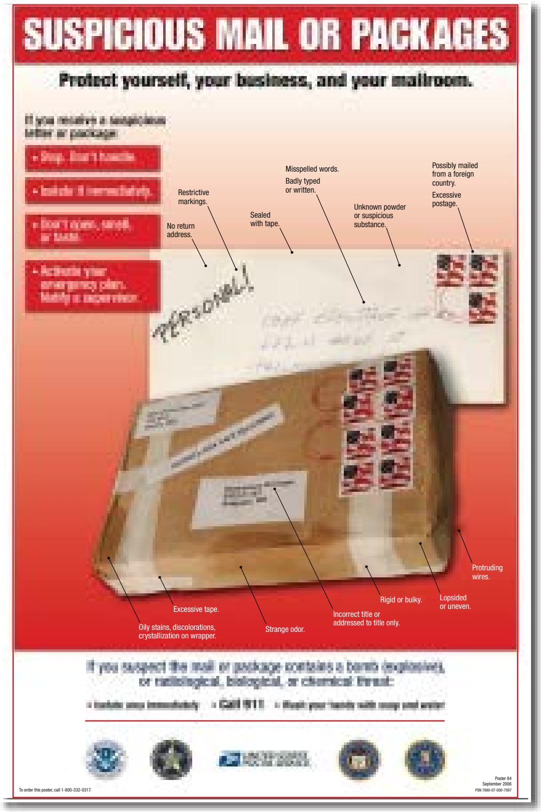
The Real Estate Information Sharing and Analysis Center is a public-private partnership between the U.S. real estate industry and Federal homeland security officials. The partnership facilitates information sharing on terrorist threats, warnings, incidents, vulnerabilities and response planning to counter terrorism and protect buildings and the people who occupy and use them. http://www.reisac.org

Real Estate Roundtable (RER)

The Real Estate Roundtable brings together leaders of the Nation's top publicly-held and privately-owned real estate ownership, development, lending, and management firms with the leaders of major national real estate trade associations to jointly address key national policy issues related to real estate and the overall economy. By identifying, analyzing, and coordinating policy positions, the Roundtable's business and trade association leaders seek to ensure a cohesive industry voice is heard by government officials and the public about real estate and its important role in the global economy. Collectively, Roundtable members' portfolios contain over 5 billion square feet of office, retail, and industrial properties valued at more than $1 trillion; over 1.5 million apartment units; and in excess of 1.3 million hotel rooms. Participating trade associations represent more than 1.5 million people involved in virtually every aspect of the real estate business. http://www.rer.org

U.S. Postal Service

The printable poster outlines the basic identification of a suspicious package and the actions that should be taken if personnel encounter such a package. http://about.usps.com/posters/pos84.pdf


SUSPICIOUS MAIL OR PACKAGES
Protect yourself, your business, and your mailroom.
If you receive a suspicious letter or package:
• Stop. Don't handle.
• Isolate it immediately.
• Don't open, smell, or taste.
• Activate your emergency plan. Notify a supervisor.
Restrictive markings.
No return address.
Sealed with tape.
Misspelled words.
Badly typed or written.
Unknown powder or suspicious substance.
Possibly mailed from a foreign country.
Excessive postage.
PERSONAL!
Protruding wires.
Lopsided or uneven.
Rigid or bulky.
Incorrect title or addressed to title only.
Strange odor.
Excessive tape.
Oily stains, discolorations, crystallization on wrapper.
If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:
• Isolate area immediately • Call 911 • Wash your hands with soap and water
To order this poster, call 1-800-332-0317.
Poster 84
September 2006
PSN 7690-07-000-7097

Appendix D: Additional Training for Security Staff

Below is a listing of additional training courses, intended to broaden your security guard force's knowledge base and supplement State-specific training requirements. The no-cost training courses listed are provided by the Department of Homeland Security's Office for Bombing Prevention, the FEMA Emergency Management Institute's Independent Study Program, and more.

Active Shooter – What You Can Do (IS-907)

This training course provides the public with guidance on how to prepare for and respond to active shooter crisis situations. The course was developed by the Office of Infrastructure Protection through a collaborative process that included representatives from the Commercial Facilities Sector and FEMA EMI. Development also included consultation with the Federal Law Enforcement Training Center. http://training.fema.gov/EMIWeb/IS/IS907.asp

Bombing Prevention Workshop

This workshop enhances effectiveness in managing a bombing incident, for regional-level stakeholders and planners within emergency management, security, and law enforcement, through analysis of current strategy development and regional best practices. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

Citizen's Guide to Disaster Assistance (IS-7)

This independent study course provides a basic understanding of the roles and responsibilities of the local community, State, and the Federal Government in providing disaster assistance. It is appropriate for both the general public and those involved in emergency management who need a general introduction to disaster assistance. http://training.fema.gov/EMIWeb/IS/is7.asp

Effective Communication (IS-242.a)

The course was aligned to the NRF and NIMS updates. Being able to communicate effectively is a necessary and vital part of the job for every emergency manager, planner, and responder. This course is designed to improve your communication skills. It addresses:

- Basic communication skills,
- How to communicate in an emergency,
- How to identify community-specific communication issues,
- Using technology as a communication tool,
- Effective oral communication, and
- How to prepare an oral presentation.

Exercises, An Introduction to (IS-120.a)

IS 120.a introduces the basics of emergency management exercises. It also builds a foundation for subsequent exercise courses, which provide the specifics of the Homeland Security Exercise and Evaluation Program (HSEEP) and the National Standard Exercise Curriculum. This course will introduce you to the following concepts:

- Managing an exercise program,
- Designing and developing an exercise,

- Conducting an exercise,
- Evaluating the exercise, and
- Developing and implementing an improvement plan.

http://training.fema.gov/EMIWeb/IS/is120.asp

Hazardous Materials, An Introduction to (IS-5.a)

This independent study course is intended to provide a general introduction to hazardous materials that can serve as a foundation for more specific studies in the future. The course has five units: *Health and Environmental Regulations, Hazardous Materials Identification Systems, Identifying Hazardous Materials, Hazardous Materials and Human Health, and Preparing for Hazardous Materials Incidents.* http://training.fema.gov/EMIWeb/IS/IS5.asp

Hazard Mitigation, Introduction to (IS-393.a)

FEMA has produced a series of courses intended to train those who have responsibility for, or interest in, reducing hazard risks in their States, communities, or tribes. This course provides an introduction for those who are new to emergency management and/or hazard mitigation.
http://training.fema.gov/EMIWeb/IS/is393a.asp

Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop

This workshop enhances participants' knowledge, skills, and abilities concerning improvised explosive devices (IEDs), and outlines specific safeties associated with bomb threat management and IED awareness, incidents, and prevention. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

Improvised Explosive Device Search Procedures

This workshop increases preparedness of security personnel and facility managers of sites that are hosting a special security event. It focuses on general safeties used for specialized search and explosives sweeps and can be tailored to meet specific participants' needs. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

Incident Command System (IS-100.b)

IS-100.b, Introduction to the Incident Command System (ICS) provides the foundation for higher level ICS training. This course describes the history, features, principles, and organizational structure of the Incident Command System. It also explains the relationship between ICS and the National Incident Management System (NIMS).
http://training.fema.gov/emiweb/is/is100b.asp

National Incident Management System (NIMS), An Introduction (IS-700.a)

IS-700.a, An Introduction to the National Incident Management System (NIMS), is a two-day course on the components of a multi-agency coordination system and establishes the relationships between all elements of the system. Upon completion, students will be able to:

- Define multi-agency coordination at the local, State, and Federal levels of government;
- Identify each agency involved in incident management activities to ensure appropriate situational awareness and resources status information is shared through multi-agency coordination;
- Identify typical priorities established between elements of the multi-agency coordination system;

- Define key terms related to multi-agency coordination systems;
- Describe the process of acquiring and allocating resources required by incident management personnel in relationship to the entire multi-agency coordination system;
- Identify typical future resource requirements for the entire multi-agency coordination system; and
- Identify potential coordination and policy issues arising from an incident relative to the entire multi-agency coordination system.

http://training.fema.gov/EMIWeb/IS/is700a.asp

National Response Framework (NRF), An Introduction (IS-800)

This course is intended for government executives, private-sector and nongovernmental organizations leaders, and emergency management practitioners including senior elected and appointed leaders, such as Federal department or agency heads, State Governors, mayors, tribal leaders, and city or county officials – those who have a responsibility to provide for effective response. This course introduces the concepts and principles for the National Response Framework (NRF). Upon completion, students will be able to describe:

- The purpose of the NRF;
- The response doctrine established by the NRF;
- The roles and responsibilities of entities as specified in the NRF;
- The actions that support national response; and
- The response organizations used for multiagency coordination.

http://training.fema.gov/EMIWeb/IS/IS800b.asp

Private Sector Counterterrorism Awareness Workshop

This workshop educates private sector security professionals about counterterrorism tactics and techniques through exposure to key elements of soft target awareness, surveillance detection, and IED recognition. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

Protecting Critical Infrastructure Against Insider Threats (IS-915)

This training course provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure.

http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-915

Protecting Your Home or Small Business From Disaster (IS-394.a)

The purpose of this course is to provide a foundation of knowledge that will enable participants to:

- Describe different types of natural disasters;
- Describe hazards that pose a risk to their home or small business;
- Explain how protective measures can reduce or eliminate long-term risks to their home and personal property from hazards and their effects; and
- Explain how protective measures for small businesses secure people, business property and building structures; and prevent business loss from a natural disaster.

http://training.fema.gov/EMIWeb/IS/IS394a.asp

Protective Measures

This course enhances commercial sector individual and organizational awareness on how to devalue, detect, deter, and defend facilities from terrorism by providing the knowledge and skills necessary to understand common vulnerabilities and employ effective protective measures. It serves as a follow-up to the *Soft Target Awareness* course below, focusing more on implementation than awareness. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

Soft Target Awareness

This course enhances individual and organizational terrorism awareness and facilitates information sharing. Commercial infrastructure facility managers, supervisors, operators, and security staff learn to be proactive and better understand their roles in deterring, detecting, and defending facilities from terrorism. Participants choose from five focus areas within the Commercial Facilities Sector: Stadiums and Arenas; Places of Worship; Education; Malls and Shopping Centers; and Large Buildings, Hotels, and Medical Facilities. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

"Soft Target Awareness: Active Threat Recognition for Retail Security Officers" Webinar

This 85-minute presentation is split into easy to understand modules and uses specific foreign and domestic case studies to explain lessons learned and discuss specific considerations for retail and shopping centers. The training discusses signs of criminal and terrorist activity, types of surveillance, and suspicious behavioral indicators. To access, please register at: https://connect.hsin.gov/attrrso/event/registration.html. After submitting the short registration information (to include setting a password of your choice) you will receive an email confirmation with instructions for logging in to view the material.

"Soft Target Awareness: Threat Detection and Reaction for Retail & Shopping Center Staff" Webinar

This 20-minute Web training session addresses the threat of explosives and firearms attacks in retail environments. It provides a basic approach to threat recognition, reporting, and reaction suitable for all "front line" retail staff. Topics covered in the Web training include basic threat awareness, staff roles and responsibilities for reporting suspicious activity and responding to incidents, identification of potential terrorist activity, and IED recognition. This Web training is available to the private sector through the Homeland Security Information Network–Critical Infrastructure (HSIN-CI). https://connect.hsin.gov/p21849699/

Surveillance Awareness: What You Can Do (IS-914)

This training course makes critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance. http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-914

Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff

This course teaches commercial infrastructure operators and security staff of nationally significant critical infrastructure facilities how protective measures can detect and deter potential threats to critical infrastructure and fundamentals for detecting surveillance activity. Participants apply skills such as vulnerability and red zone analysis, surveillance detection, and observation and reporting during practical exercises. For more information, contact your local Protective Security Advisor or OBP@dhs.gov.

Workplace Security Awareness (IS-906)

This training course provides guidance to individuals and organizations on how to improve the security in your workplace. http://training.fema.gov/EMIWeb/IS/is906.asp