Protective Measures Guide for the U.S. Outdoor Venues Industry

June 2011

Homeland Security

Homeland Security

Protective Measures Guide for the U.S. Outdoor Venues Industry

June 2011

Prepared by:
Commercial Facilities Sector-Specific Agency
Sector-Specific Agency Executive Management Office
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

The Office of Infrastructure Protection (IP) is a component within the National Protection and Programs Directorate. IP leads the coordinated national program to reduce risks to the nation's critical infrastructure posed by acts of terrorism, and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. Visit www.dhs.gov/criticalinfrastructure.

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 18 critical infrastructure sectors designated by the Department. Within the CF Sector, the Outdoor Venues Subsector represents entities that provide the public with places to meet and gather in outdoor spaces for the purposes of entertainment, education, and recreation. 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 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-Specific Agency Executive Management Office (SSA EMO) CF Branch for commercial facilities. Serving as the Sector-Specific Agency (SSA) for the CF Sector, the CF Branch 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 been working to produce a suite of protective measures guides that provide an overview of best practices and protective measures designed to assist owners and operators in planning and managing security at their facilities or events. The *Protective Measures Guide for the U.S. Outdoor Venues Industry* is one of these guides and reflects the special considerations and challenges posed by the Outdoor Venues Subsector.

For more information on IP and SSA EMO please visit http://www.dhs.gov/criticalinfrastructure.

DHS received input from private sector owners and operators, and the following associations and law enforcement agencies in the preparation of this guide:

- U.S. Secret Service
- Federal Bureau of Investigation
- New York Police Department
- International Association of Venue Managers
- International Festivals & Events Association
- World Waterpark Association

This *Protective Measures Guide for the U.S. Outdoor Venues Industry* is designed to provide venue owners and operators with information that can be used to maintain a safe environment for patrons and employees. The measures provide suggestions for successful planning, organizing, coordinating, communicating, operating, and training activities to augment the overall security posture at outdoor venues.

Section 1 - Outdoor Venues Profile

- Identifies key vulnerabilities associated with different types of outdoor venues or activities.

Section 2 - Terrorist Objectives

- Discusses motivations behind terrorist attacks.

Section 3 - Threats and Hazards

- Identifies scenarios that could impact an outdoor venue and provides real-life examples of incidents.

Section 4 - Protective Measures

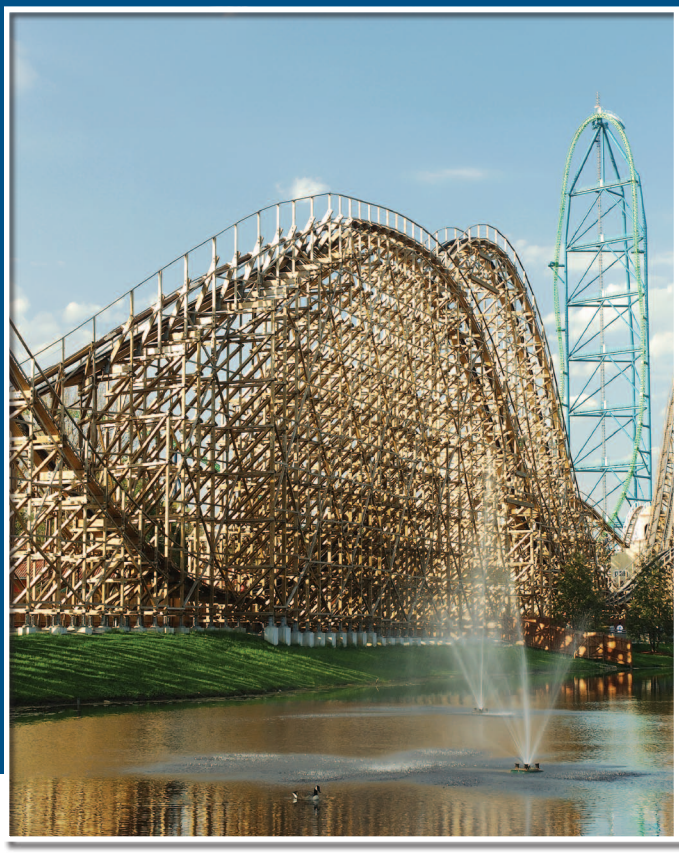
- Provides a compendium of non regulatory protective measures.

Appendices to this guide identify additional tools and resources in the form of posters, checklists, documents, training opportunities, Federal programs, and Web sites that may further assist an owner or operator in assessing vulnerabilities and developing appropriate protective programs.

Please note the following with regard to the suggested protective measures in this guide:

- This guide is not a complete source of information on protecting outdoor venues. Owners, operators, and security personnel should leverage the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.
- The protective measures outlined in this document are presented for guidance purposes only. They are not a requirement under any regulation or legislation.
- Not all suggested protective measures will be relevant or applicable to all specific outdoor venues because of the wide variety in types, sizes, and locations of venues. The ability to implement them at any specific outdoor venue will vary considerably.

1. Outdoor Venues Profile



Outdoor venues encompass a wide range of facilities and activities. For the purpose of the following overview, outdoor venues are divided into two general categories: 1) parks (e.g., amusement, theme, and water), fairgrounds, and other fixed facilities with an established perimeter; and 2) outdoor gatherings (e.g., festivals in an open park, parades, and flea markets) that are held in more open areas.

1.1 Outdoor Venues Overview

1.1.1 Parks, Fairgrounds, and Other Fixed Facilities with an Established Perimeter

Amusement parks, theme parks, and fairgrounds often include rides and other attractions and activities assembled to entertain large groups of people. As compared to a traveling fair or carnival, these parks have a fixed location. Attendance at amusement and theme parks varies widely, with some having an annual attendance in the range of 100,000 while other larger, more established theme parks can attract more than 10 million visitors per year.

Theme parks and amusement parks usually cover a considerable land area and, as a result, have an extensive perimeter. Wide pedestrian walkways allow easy access to rides and attractions within the site. Service roads, parking areas, and public access roads typically allow vehicle access to points near the theme park's rides, attractions, and perimeter. Larger parks may operate trams, shuttle buses, monorails, or other corporate-owned transportation systems. Some parks may be located adjacent to public transportation hubs.

A variety of structures including rides, restaurants, shops, entertainment halls and stages, and service buildings are usually present. Rides and attractions often incorporate physical and/or psychological experiences utilizing heights, sounds, and sights. Theme parks may also incorporate hotels and meeting facilities, and entertainment districts that include shops, arcades, movie theaters, shows, and restaurants. These may be on the same or adjacent grounds. Larger parks may be nationally or internationally known and have icons which patrons associate with the park.

"Theme parks may also incorporate hotels and meeting facilities, and entertainment districts that include shops, arcades, movie theaters, shows, and restaurants."

Fairgrounds most typically refer to a permanent space that hosts fairs, most often a state fair, as well as other activities. Fairgrounds may have amusement park-style rides at scheduled times during the year. They may involve temporary structures, such as tents, tables, and booths, and they can include exhibits of everything from crafts to livestock. In addition to large open spaces, the grounds may include barns, administration buildings, theaters, exhibition and convention halls, stadiums, sports fields, and museums.

Although summer is traditionally the high season for parks and fairgrounds, some parks are finding new sources of revenue by extending their seasons into autumn. Other parks may be open year round. Exhibition halls, theaters, stadiums, sports fields, and other buildings at fairgrounds are used year round.

1.1.2 Outdoor Gatherings

Outdoor gatherings can occur on downtown city streets, regional parks, and other outdoor venues. They include celebrations, concerts, demonstrations, fairs, festivals, flea markets, parades, protests, and rallies. They can be local, regional, or national events.

At some large outdoor public gatherings, such as rallies or concerts, individuals are typically concentrated in a particular location.

At parades or demonstrations, for instance, people line roadways, march down streets, or ride in a vehicle down a parade route. At fairs and festivals, people are constantly moving from one location to another within a particular site. In many of these cases, there may be no protected perimeter, unless it is a ticketed event and has strict access control measures.

In many cases, large outdoor public gatherings involve temporary structures, such as tents and booths with exhibits displaying everything from antique collectibles to military equipment to livestock. Unlike events at fixed facilities, large outdoor public gatherings may not rely on a permanent allocation of dedicated security resources. Therefore, almost all aspects of security must be planned and formulated for each individual gathering. In addition, event organizers and supporters may be unpaid volunteers rather than regular, part-time, or contracted employees.

Any organization or group can be involved in arranging a large outdoor public gathering. For example, large corporations sponsor free concerts; political parties arrange rallies; civic organizations stage parades; advocacy groups hold demonstrations; commercial enterprises organize fairs and festivals; and people spontaneously congregate to celebrate events. In many cases, government agencies also participate in securing these types of gatherings.

Finally, many outdoor gatherings require special permits and may place a strain on limited community resources. Each community's laws, ordinances, and permitting process are different.

"Therefore, almost all aspects of security must be planned and formulated for each individual gathering."

1.2 Key Vulnerabilities

Vulnerabilities will differ by specific characteristics and circumstances of the outdoor venue. Among the key vulnerabilities of the outdoor venues industry are the following:

- Open access: Many outdoor public gatherings have no access controls. Although many events have a significant security presence, the ability to monitor the crowd, including what items can be carried into the venue, is limited. Some outdoor gatherings may have gated areas (e.g., entertainment stage, parade viewing stand) where participants may be screened and additional security measures may be in place, but the ability to provide substantial control over participants in an outdoor gathering may not be possible.

  Openness to the general public is an important element for successful business operation at parks and fairgrounds. Although parks typically have gates and other access control measures, venue management personnel are interested in minimizing the time guests have to wait in lines to enter the park. In addition, screening and searches may detract from the recreational experience and positive customer perception, thus making the park more vulnerable to prohibited and illegal items being brought onto the premises.

- Large congregations of people: Outdoor gatherings have large congregations of people, often over a wide area. Parks and fairgrounds have many places where large crowds gather (e.g., waiting for admittance to rides, ticket lines), which can provide an opportunity for adversaries to inflict a large number of casualties.
- Multiple locations to place explosives or hazardous agents: Large outdoor public gatherings are congested, often noisy, and frequently disorganized. A determined adversary can take advantage of this environment to hide a package containing dangerous materials or discharge a weapon or explosive. Parks and fairgrounds are complex facilities with many trash containers, restrooms, shops, theaters, etc., that offer locations where explosives or hazardous agents could be placed unobtrusively and may be difficult to find quickly.
- Operating with a staff of temporary employees and volunteers: The use of part-time or temporary employees, as well as the large number of volunteers at many outdoor gatherings, may limit the ability of event sponsors to conduct background screening for all staff. In addition, seasonal staff and high staff turnover provide challenges in providing training on security measures.
- Evacuation difficulties: Rapid evacuation of park patrons in the event of an incident can be difficult due to restricted entry/exit points over a large area, the presence of large numbers of children, and difficulty in communicating evacuation instructions over the expanse of the park. There are few places to take shelter when hazardous weather, including lightning, requires that patrons to evacuate or take shelter. Patrons may not be able to clearly hear instructions over a public address system in an outdoor setting over a noisy crowd. In the case of open fairs and festivals, a public address system may not be present.
- Access to peripheral areas: There are limited controls on vehicles traveling into and through areas contiguous to large public gatherings. For parades, vehicles are sometimes allowed to cross the parade route during breaks.

2. Terrorist Objectives

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

Terrorist organizations have demonstrated an understanding of the potential consequences of carefully planned attacks within the United States. Their motivations include, but are not limited to, advancing ideological and political agendas addressing 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 illnesses 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 the operation of the facility or releasing hazardous materials to the surrounding area. Likewise, deteriorating public morale and confidence in a facility's security following an incident produces

an ongoing psychological impact that expands the economic losses of a facility as a result of the reputational harm suffered. Just as significantly, inflicting psychological trauma upon segments of the consumer population is an objective for many terrorists, as it curtails participation in activities that terrorists oppose. It is important for owners and operators to understand terrorist motivations and objectives that that may lead to attacks against the Nation's critical infrastructure, including outdoor venues, so they may take appropriate protective measures to reduce risk and increase resilience at their facilities and gatherings.

3. Threats and Hazards

The best way to manage risk is to understand an outdoor venue's potential vulnerability to threats and hazards and train security personnel and staff to recognize and report potentially significant incidents. The threats and hazards described below are not solely linked to outdoor venues. Many other facilities face the same threats and hazards and share many of the same vulnerabilities. The purpose of this document is not to identify and prioritize what threats and hazards are specific to outdoor venues, but rather to provide decisionmakers at outdoor venues examples and scenarios that may impact their specific venue.

For the purposes of this guide, manmade hazards are acts of terrorism, or 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. [1] Manmade hazards are distinct from hazards involving human error or negligence, which are defined as "accidents" (Section 3.2).

> "The threats and hazards described below are not solely linked to outdoor venues. Many other facilities face the same threats and hazards and share many of the same vulnerabilities."

[1] From Department of Homeland Security Office of Inspector General, FEMA's Progress in All-Hazards Mitigation, October 2009, p. 2, *www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-03_Oct09.pdf*, accessed February 21, 2011.

3.1 Manmade Hazards

These attack methods are the manner and means an adversary may use to cause harm to a target. Terrorists 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

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

For example, an abandoned backpack containing a bomb and heavy shrapnel was discovered by city workers on the parade route prior to a Martin Luther King Jr., Day Unity March in Spokane, Washington, in January 2011, and a Michigan golf course was evacuated when three tennis-ball sized devices were found on the course in June 2010.

3.1.2 Vehicle-Borne Improvised Explosive Devices

Vehicle-borne IEDs (VBIEDs) are improvised explosive devices that are loaded into a car or truck or onto a motorcycle. 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. VBIEDs are a common means of attack throughout the world. Surveillance by the terrorist(s) often precedes IED and VBIED attacks.

VBIEDs are used commonly as a weapon of choice by terrorists. 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 under the age of 6, 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. Two more recent examples of the attempt to use a VBIED involve outdoor venues. In May 2010, an attempt was made to detonate a crudely made gasoline and propane bomb in a Nissan Pathfinder on a busy Saturday night in Times Square. The bomb did not explode, and a street vendor who spotted smoke coming from the vehicle alerted the police, who cleared the area. In November 2010, a man was arrested by the FBI in Portland Oregon after he attempted to detonate what he believed to be an explosives laden van that was parked near a tree lighting ceremony in Portland's Pioneer Courthouse Square. The arrest was the culmination of a long-term undercover operation.

3.1.3 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. In five coordinated attacks, the perpetrators, a Japanese cult group called Aum Shinrikyo, released sarin on several lines of the Tokyo Metro, killing thirteen people, severely injuring fifty and causing temporary vision problems for nearly a thousand others.

3.1.4 Biological Attack

Biological pathogens such as anthrax and plague can cause disease and are used by terrorists because of their ability to cause mass casualties while exhausting emergency response resources. Biological agents can be dispersed in the atmosphere via crop-dusting aircraft or other airborne medium; introduced 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.

There are some prominent examples of this threat that have taken place within the United States. One such incident was the contamination of salad bars with Salmonella by a religious cult, the Rajneeshee in 1984. The group deliberately contaminated the salad bars at 10 local restaurants, which left 751 people ill in Dalles, Oregon. Another example is the distribution of letters containing anthrax. Letters containing anthrax spores were mailed to several news media offices and two U.S. Senators, killing five people and infecting 17 others in 2001. This incident received a lot of media attention and created fear across the country.

3.1.5 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 venue directly or through the HVAC system if there are buildings present.

An example of a radiological attack that gained media attention was the murder of Alexander Valterovich Litvinenko, a former Soviet KGB officer. On November 1, 2006, Litvinenko suddenly fell ill and was hospitalized in what was established as a case of poisoning by radioactive polonium-210, resulting in his death on 23 November.

3.1.6 Aircraft Attack

Terrorist can and have previously demonstrated the ability to leverage aircraft of any size to deliver attackers, explosives, or hazardous materials to a target area or facility. The aircraft themselves can also be used as a weapon.

There are two significant examples of this attack methodology in recent history. Most notably 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 pilot furious with the Internal Revenue Service crashed his small plane into an Austin, Texas, seven-story office building. Nearly 200 Federal tax employees were employed in that building.

3.1.7 Maritime Attack

Ships and boats of various sizes can be used to deliver attackers, explosives, or hazardous materials. The vessel itself also can be used as a weapon. On October 12, 2000, The USS Cole suffered a suicide attack against while it was harbored and refueling in the Yemeni port of Aden. Seventeen American sailors were killed, and 39 were injured. This event was the deadliest attack against a United States Navy vessel since 1987. The terrorist organization al-Qa'ida claimed responsibility for the attack.

3.1.8 Cyber Attack

Malicious and non malicious actors can infiltrate data processing, transfer, storage, communications, security and surveillance systems to cause economic and operational damage and 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 information systems may also result in disruption to, or misinformation about, facilities, mechanical systems such as rides, and emergency communications, potentially endangering patrons or employees. Symantec Corp. reported that, in 2009, 75 percent of organizations suffered a cyber attack and lost an average of $2 million annually. The report is based on a survey of respondents from a wide variety of industries from 27 countries including 300 U.S. organizations.

3.1.9 Sabotage (Including Insider Threat)

The disruption, damage, or destruction of a venue through sabotage, and the introduction of hazardous materials into the facility are of concern. Sabotage can be perpetrated by employees or by outsiders. 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.

3.1.10 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.

The use of small arms is becoming a more common tactic for terrorists as well as criminals. An active shooter incident can strike anywhere, as seen more and more often in the news. Two recent incidents include a June 2009 incident in which a guard was killed when a gunman opened fire in the U.S. Holocaust Museum and an April 2007 incident in which a student opened fire and killed 32 and wounded many others at a university in Blacksburg, Virginia.

3.1.11 Arson

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. For example, in February 2009, arsonists started three separate fires at the Whakapapa Ski field. The fire destroyed a café and a workshop containing expensive snow grooming equipment. The fire also damaged the structure housing the ski chair lift mechanism. Arson is a tactic often employed by animal and environmental extremists.

3.2 Accidents

Outdoor venues 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 outdoor venues. For example, in May 2010, a fire in a manufacturing plant that used cyanide led to the evacuation of a nearby flea market in Florida, as a precaution, and in June 2010, a eight-ounce canister of butane fuel, left out in direct sunlight, exploded at a street festival in a Chicago neighborhood, injuring three people.

3.3 Natural Hazards

A natural hazard such as a hurricane, tornado, earthquake, flood, or severe storms may occur without warning and severely impact operations at an outdoor venue.

3.3.1 Extreme Weather

Weather conditions can have a major impact on both safety and business operations at an outdoor venue. Most outdoor venues have limited indoor facilities that could be used as a shelter. Tornadoes, heavy rain, hail storms, lightening, high winds, and flooding are the weather conditions most likely to impact operations. Rains and flash floods killed 16 people at a campground in Arkansas in June 2010. In June 2002, a violent storm killed one person and injured nearly 50 at a Pennsylvania amusement park.

3.3.2 Pandemic

A pandemic is a sudden outbreak of an infectious disease that spreads through human populations across a large region. Over the last few years there have been rising concerns over the likelihood of a pandemic. In June 2009, the World Health Organization announced that the H1N1 virus had met the definitional threshold of a pandemic. In 2009, Mayfest in Fort Worth, Texas, was cancelled because of concern over the spread of the H1N1 virus. The cancellation cost the organizer half a million dollars.

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 terrorists; 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. Venue 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 decision making process, a risk-based protective posture is recommended. DHS recognizes three factors to calculate 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 vs. 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 outdoor venue 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 of outdoor venues are also encouraged to have a scalable approach to managing risk. The capability to increase protective measures based upon the threats to their property 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.

“Venue 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.”

The protective measures described in this chapter are designed to provide information and assistance to outdoor venue owners and 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
- Access Control
- Credentialing
- Signage and Notification

- Barriers
- Communication and Notification
- Monitoring, Surveillance, Inspection
- Information Security/Cybersecurity
- Infrastructure Interdependencies
- Food and Beverage Services
- Special Considerations – Hazardous Weather

Protective measures that are recommended for use during periods of high alert, when a higher state of readiness may be required at a property, facility region, or all outdoor venues nationally are given at the end of each section.

4.1 Planning and Preparedness

Operators of outdoor venues that attract large crowds are responsible for assessing their specific vulnerabilities and practicing the best and most cost-effective mitigation strategies for their own unique security needs. This assessment includes development, implementation, and coordination of plans and programs to ensure security and emergency preparedness. For fixed venues, some of the measures may be implemented on an ongoing or periodic basis. For some outdoor gatherings, the measures must be formulated for the particular event. Owners and operators should consider the following planning and preparedness steps:

Security and Personnel Responsibilities and Coordination

- Designate an experienced person as Security Director/ Emergency Preparedness Coordinator to develop, implement, and coordinate all security-related activities.
- Involve venue operators, security personnel, local police and other government services, including local fire, emergency management, and emergency services departments at several levels in security planning. You may want to also consider involving other department leads such as marketing and communications.
- Clarify agency emergency response responsibilities and other responsibilities related to venue security and emergency response. Develop Memoranda of Understanding (MOUs) or Memoranda of Agreement (MOAs) between venue management and relevant Federal, State, and local emergency response agencies.
- Establish liaison with the FBI, DHS, State Homeland Security Advisors, additional emergency management agencies, public health organizations, and industry organizations to enhance information exchange, track threat conditions, and support investigations. For example, every FBI Field Office has a Special Events Coordinator and a Weapons of Mass Destruction Coordinator who may be able to provide resources and awareness to your venue and team.

- 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, location of stages, buildings, rides, emergency access routes, first aid stations, concession areas) with local police, fire, and emergency management agencies. In addition, share relevant information, including interior layouts of dark rides, locations of hazardous materials, and locations of fire hydrants. Restrict access to this venue data to these public safety agencies and determine how sensitive information will be handled in their agencies.

Assessments

- Work with local law enforcement and the local FBI field office 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.

- Consider the following to determine the most likely threats to the outdoor venue:
  - Determine whether there is a history of a threat type in the area or within the industry, and whether there are trends regarding outdoor venues that will affect the likelihood of an incident.
  - Evaluate the visibility or symbolic importance of the venue and determine whether an adversary would seek to attack based on the symbolic importance (e.g., a theme park is nationally and internationally known; a large outdoor gathering is scheduled on a date of significance; or the nature of the gathering, participants, or location are significant or controversial).
  - Identify and assess other activities and operations (e.g., airports, chemical plants, government buildings, pipelines, rail lines) in the vicinity to determine whether an incident at a nearby facility or infrastructure could pose a hazard to the outdoor venue. Exchange contact information with managers of such facilities and maintain a list of contacts.
  - Determine whether there are crime trends including gang activity that could affect the likelihood of an incident at the venue.
  - Identify adversarial groups and their threat capabilities.
  - Identify the most logical venue threats (e.g., bomb, person with firearms, chemical/biological agent, and suspicious package).
  - Identify dignitaries or other high profile attendees who may be the target of specific threats.
  - Identify particular activities, such as a concert, and areas (e.g., podium, viewing stand, or rides) that may be subject to a specific threat or have enhanced visibility (e.g., may be televised).

- Evaluate natural hazard trends and identify the threats that would cause the venue to be evacuated or for patrons to shelter in place. Evaluate the probable amount of warning time for the hazard. There may be minimal or no warning for lightning or a tornado, but 24 hours or more for a hurricane.

❍ Conduct a vulnerability assessment to evaluate the threats to the venue and identify areas of weakness that could result in serious consequences. Consider the following:

- Determine the physical features or operational attributes that may leave the venue 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, ability to monitor items carried into the venue, open parking areas with limited security controls, difficulty hearing emergency or evacuation announcements due to large noisy crowds).
- Determine appropriate vulnerability assessment strategy (e.g., self-assessment, Federal- or State-led assessment, expert reviews, or third-party assessment) and methodology.
- Identify and group vulnerabilities using common threat scenarios.
- Analyze the benefits of existing protective programs.
- Assess residual gaps in security or planning to determine unresolved vulnerabilities.

❍ Evaluate the impact of the outdoor venue on the surrounding area. For example, crowds and street closures associated with a special event may impact businesses and homeowners in the vicinity. Owners of retail stores, restaurants, and other small businesses should know what to expect during normal operations or during special events such as a special concert drawing extra crowds). Meet with businesses to discuss potential problems and to obtain input from the surrounding community.

Emergency Preparedness

❍ Develop an Emergency Response Plan for the venue. Develop this plan in concert with public safety and response agencies.

❍ As part of the Emergency Response Plan, develop standard operating procedures and checklists to cover potential emergencies, including but not limited to:

- Bomb threats
- Fire or explosion
- Suspicious vehicle, item, or package
- Power failure
- Severe weather
- Hazardous material or chemical spill
- Active shooter

- Work with the local emergency management agency to address procedures for dealing with people with special needs during an emergency. Consider FEMA's *Comprehensive Preparedness Guide 301: Interim Emergency Planning Guide for Special Needs Populations*[2] as a resource.
- Establish procedures for event delays and for shutting down the venue and evacuating the grounds in the event that a threat is deemed too serious to continue the event or operation of the venue. Consider the local transportation system (e.g., mass transit, streets, and highways) in evacuation planning. Consider roadway traffic patterns and whether people can get out and emergency responders can get in.
- Develop procedures to shelter in place if buildings and other suitable structures are available.
- Develop procedures to address readmission of guests if the need to evacuate is temporary.

- Establish a threat response protocol for when the venue is open to the public and during off-hours:
  - Identify persons internal and external to the facility to be notified and the order in which they should be notified. Ensure the notification list is current.
  - Develop procedures for dealing with hoaxes and false alarms so they will not impact venue activities.
- 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.

- Identify the chain-of-command relative to responding to manmade or natural incidents and roles, responsibilities, and phone numbers for the decision makers. The authority includes actions such as halting activities at the venue, evacuating the area, or coordinating shelter-in-place, if there are buildings on the premises or nearby.
- Develop flow charts showing the means of communicating decisions and information from the top decisionmaker down to the attendees. Describe primary and backup communication systems such as phones, radios, jumbo screens, and public address systems.
- Develop audio and video scripts such as public address announcements for specific emergency announcements, including but not limited to natural disasters, weather, bomb threats, and other incidents.

[2] 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/, accessed February 21, 2011.

- ❍ Retain copies of the Emergency Response Plan and supporting documentation in redundant locations. Ensure that key personnel have access to these plans.
- ❍ Establish procedures, as part of the Emergency Response Plan, to implement additional protective measures as the threat level increases. In addition, establish procedures for returning to lower security levels as the threat decreases.
- ❍ Consider third-party evaluation and verification of the Emergency Response Plan.

- ❍ Ensure that equipment and supplies are available to support emergency response requirements, including:
  - Storing emergency supply kits in areas where they are accessible to employees or emergency responders.
  - Determining the need for personal protective equipment (PPE) for employees (e.g., breathing apparatus).

Security Preparedness

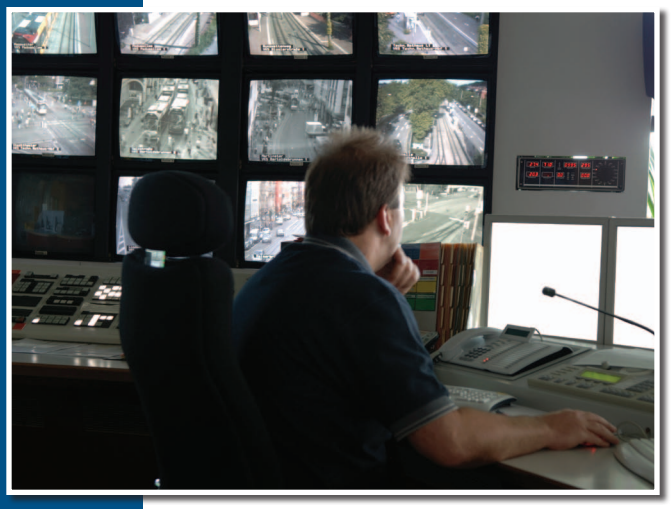
- ❍ Conduct training exercises with employees and volunteers to practice the security and emergency response plans to ensure there are adequate resources available to implement the plan and that all venue operation units can implement their responsibilities under the plan.
- ❍ Conduct training and exercises with law enforcement and emergency responders to familiarize them with the venue and its security and emergency procedures.
- ❍ Conduct after-action reviews for exercises and revise procedures, as needed.
- ❍ Consider volunteering the outdoor venue as a training-ground during the off-season (or off hours for venues that are open year-round), so that local emergency response agencies are familiar with the venue if an emergency occurs.
- ❍ Establish a location for an Emergency Operations Center in order to manage the security and safety aspects of activities during an incident. Designate a backup location in the event the emergency operations center is disabled. Consider the use of a mobile command center.
- ❍ Develop security plans and procedures to be scalable to the threat to your venue. When the threat level is elevated as a result of a credible threat to your venue, geographic area, or industry or based on hosting a high risk/high profile event, plans and procedures should provide options for increasing your security posture.

In the event of a credible threat to your venue, geographic area, or industry:

- ❍ Review and implement actions specified in security and emergency response plans.
- ❍ Activate the emergency operations center.
- ❍ Review available threat information to determine whether the venue should be closed or should be operated with reduced activities.

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 security plans and the emergency response plan.
- Maintain a record of security-related incidents. Review regularly to identify patterns or trends. Implement procedures for capturing lessons learned and revising response plans after an incident.
- 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.
- Review incident command procedure for responding to an event with local law enforcement, emergency responders, and other government agencies.
- Establish an emergency operations center or emergency command center that can be used to manage safety and security aspects of the venue and to coordinate resources during an incident.
- Determine who will staff the emergency operations center. Staffing may include: Security Director, potential Incident Commander(s), police, fire fighter/EMS personnel, venue management (operations and security), and private security. Ensure that everyone working within the emergency command center understands the protocol and resulting chain of command for handing an issue over to the appropriate government/public safety department.
- Check the status of all emergency response equipment and supplies on a regular basis. Have emergency supplies located in areas where employees can have ready access to them. Regularly inspect and replace items such as batteries, flashlights/glow sticks, bull horns, emergency vests, and battery operated radios.
- Develop a list of personnel who are approved to enter the venue after an incident and assist with recovery activities.
- Review procedures for evacuation and shelter-in-place (for venues that have suitable buildings).

In the event of a credible threat to your venue, geographic area, or industry:

- Review and implement actions specified in the security and emergency response plans. Adjust as necessary to deal with the specific incident conditions.
- Activate the venue's emergency operations center.
- Add and preposition emergency response personnel and equipment to locations that would enable rapid response to an incident.

4.3 Personnel

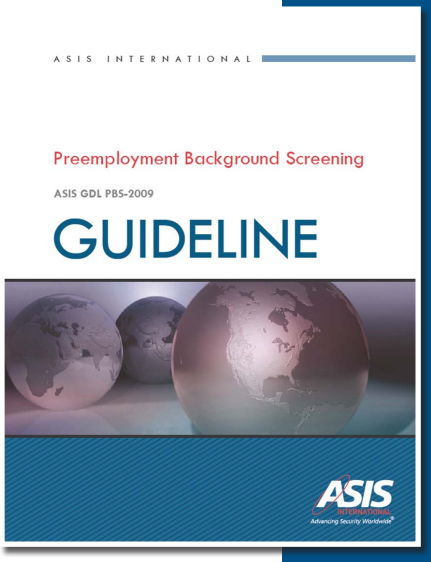
Trained and attentive staff members are an essential element of a successful protective measures program. Employees, contractors, and volunteers should be encouraged to be alert to suspicious activity and out-of-place items. Emphasize the fact that security is a responsibility for all staff and volunteers at the outdoor venue, not merely for security staff, and make it easy for personnel to raise concerns and to report their observations. Hiring a competent and credible staff is just as important to protecting an outdoor venue 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.

The nature of the outdoor venues industry creates some special situations with regards to hiring and training staff. Some amusement parks, theme parks, and fairgrounds may have fewer full-time, regular employees because these venues may not operate year-round. At some state fairgrounds and festival grounds or community gatherings, people working on the premises may be volunteers or temporary employees. The role that volunteers and temporary employees play will influence staffing and training activities.

The following measures may be considered regarding staffing issues:

Employees

- Establish an employee background screening for outdoor venue employees. Consider verifying identity, employment history, criminal convictions, financial history, and history of overseas criminal activity. The ASIS International *Preemployment Background Screening Guideline*[3] is a resource that aids U.S. employers in understanding and implementing the fundamental concepts, methodologies, and related legal issues associated with preemployment screening of job applicants and is available for purchase online.
- Conduct more detailed checks on those who will have access to critical or restricted areas, access to hazardous materials, or anyone whose duties put them in contact with children (e.g., staffing the lost children's booth or assisting children on rides).
- Develop a list of disqualifying factors that can be used to reject an individual for employment.



- Incorporate security awareness and appropriate response procedures for security situations into employee training programs. Include the following in the training:
  - Instructions for maintaining alertness to and being able to recognize situations that may pose a security threat (e.g., suspicious behaviors, persons without proper employee identification, persons carrying unusual packages, gang signs and symbols, unattended/suspicious vehicles and packages, and strange odors or liquids).

[3] Preemployment Background Screening Guideline, *www.asisonline.org/guidelines/published.htm*, accessed February 21, 2011.

- Instructions for maintaining alertness to surveillance activities that could be an indicator of potential terrorist attack (e.g., persons parking, standing, or loitering in the same area over a multiple-day period; significant interest being taken near parking areas, entrances, and areas where trams or buses discharge passengers; and persons questioning venue employees about venue operations and security routines).
- Contact and notification protocols for suspicious situations and emergencies.
- Caution in providing venue information to outsiders.
- Procedures to provide for the safety of employees during a security incident including searches, emergencies, and evacuations.
- Appropriate actions in the event of a bomb threat. Provide checklists and training to employees answering the phone for dealing with phone threats. An example of a Bomb Threat Checklist is provided in Appendix B.

- Train all employees on suspicious activity reporting. Consider incorporating information from the DHS "*If You See Something, Say Something*" initiative 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.
- Review personnel files of recently terminated employees to determine whether they pose a security risk.

Contractors, Vendors, Temporary Employees

- Provide security information and training to contractors, vendors, and temporary employees at the venue. 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.
- 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.

Volunteers

- Provide security information and training to volunteers. Advise them to be alert to suspicious activity or items and gang signs and symbols, and train them on how to report such incidents.
- Consider asking the local police to provide a security awareness training overview to volunteers, as well as employees and contractors.

- Conduct background checks on any volunteers who will have access to critical or restricted areas or anyone whose duties put them in contact with children, e.g., staffing the lost children's booth or assisting children on rides.

Security Staff

Some outdoor venues such as parades and festivals in open public parks may rely on local law enforcement for security needs. The following measures may be considered for venues that employ their own security staff:

- Maintain an adequately sized, equipped, and trained security staff based on the threat that is specific to your venue. Ensure adequate security personnel are on duty or on call in the event of an incident. Determine availability of security reinforcements that can be deployed during heightened threat conditions or in response to an incident. Conduct background checks on all security force personnel.
- Coordinate security staff operations with local law enforcement and, as needed, with State and Federal agencies such as the FBI, DHS, and the Joint Terrorism Task Force.
- Provide additional security measures (e.g., personal security specialists) or bolster existing security measures when high-profile individuals visit the venue. 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.
- Conduct regular training drills and exercises with security staff in coordination with local, State, and Federal emergency management authorities. Involve local law enforcement and other agencies as appropriate.
- Develop a procedure and location for detaining and questioning persons acting suspiciously and/or violating security regulations. Train security personnel in appropriate methods for handling these people and for identifying and confiscating sensitive items such as firearms and illegal drugs.
- Develop a security staff schedule that includes random patrols of venue.

In the event of a credible threat to your venue, geographic area, or industry:

- Update employees, vendors, and volunteers about the rising threat. Provide refreshers on Standard Operating Procedures (SOPs) to be used in different types of incidents.
- Increase security staff presence by using additional personnel or overtime. Increase patrols of remote parts of the venue and the outer perimeter.
- If necessary, request security staff support from local law enforcement. Position law enforcement officers and vehicles at entrances where they are visible to patrons entering the venue.

4.4 Access Control

Access control measures can pertain to the physical access to an outdoor venue by guests, employees, contractors, vendors, temporary employees, volunteers, vehicles, and mail and other deliveries. Measures will vary considerably by the type of venue. Fixed outdoor venues with an established perimeter such as fences and gates will have more options to control access than an open street or public park.

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., control rooms, communications centers, computer server rooms, shipping areas, mail rooms, fuel or chemical storage tanks, utility service areas, mechanical equipment for rides, staging areas, entertainment stages, food storage areas, viewing stands for dignitaries) that require special access controls. Where possible, locate sensitive equipment and assets in the interior of the venue.
- 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.
- Identify an area extending out from the venue 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.
- Coordinate with local agencies to establish emergency access lanes for fire, police, and EMS personnel. Allow emergency services vehicles to be parked near entrance points and near critical assets or areas to ensure timely response to an incident.
- Keep crowds at access points to a manageable size. Use pedestrian railings to ensure orderly control of crowds at entrances to the venue, ticket counters, and areas within the venue where large numbers of people gather (e.g., entrances to rides and entertainment stages).
- Use rope lines to open up or close off selected areas to pedestrians, as needed.

- Coordinate with law enforcement to arrange for law enforcement vehicles to be parked near entrance points and near critical assets or areas. Post uniformed police officers at key access points to observe suspicious behavior.
- Under special circumstances, and determined by law, examine the need for establishing restricted air space to prohibit aircraft flying over the outdoor venue. Coordinate with your State Homeland Security Advisor and Federal and local aviation officials about implementing these temporary flight restrictions.

Vehicles and Parking

- Ensure that parking areas provide standoff from where crowds of people gather and critical areas.
- Review vehicle traffic patterns around and inside the outdoor venue. To the extent possible, keep vehicles distant from areas where large numbers of people congregate.
- 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 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 with a definite need to be in the area, those that have been positively identified, and those that have been inspected.
- Positively identify vehicles and drivers that enter the venue. Maintain a log of all vehicles entering the premises (see Deliveries section below). 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 venue.
- 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.

Deliveries

- Limit delivery times. Schedule as many deliveries as possible for times when the venue is not open to the public, such as the early morning. For deliveries to outdoor gatherings that must be made on event days, schedule the delivery during times of non occupancy (e.g., prior to when the event begins or after the event closes).
- Accept deliveries and shipments only from known shippers, vendors, or customers.
- Consider requiring that delivery vehicle drivers, helpers, and passengers to produce a photo ID and sign in at a control point.
- Reserve the right to inspect or reject any delivery.
- Consider escorting delivery vehicles to the area within the venue where the delivery is made.
- See Food and Beverage Services (Section 4.12) for special considerations for food and beverage deliveries.

Employees, Contractors, Vendors, Temporary Employees, and Volunteers

- Issue identification badges to employees (see Section 4.5 Credentialing). Require all employees, contractors, vendors, temporary employees, and volunteers to display badges at all times. Collect identification badges at the end of their service.
- Practice the response of employees to any person without a badge in a restricted area of the venue. 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.
- Escort all non employees when they are in sensitive or critical areas.
- Assess the need for checking personal items, such as bags, when coming into or leaving the venue property.

Buildings, Rooms, Shipping/Receiving Areas, Storage Facilities, Utility Access

- 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 such as manholes and HVAC systems, hazardous materials (e.g., fuels, chemicals), and other areas where access is to be limited. Add intrusion detection systems and alarms as appropriate.
- Utilize higher security controls such as card swipe locks in sensitive or critical areas of venues that have buildings and other permanent facilities. Maintain audit trail of those accessing these areas.
- 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.
- Implement key control procedures. Track holders of all keys. Secure master keys. Require that terminating employees and contractors who have completed their work return all keys.

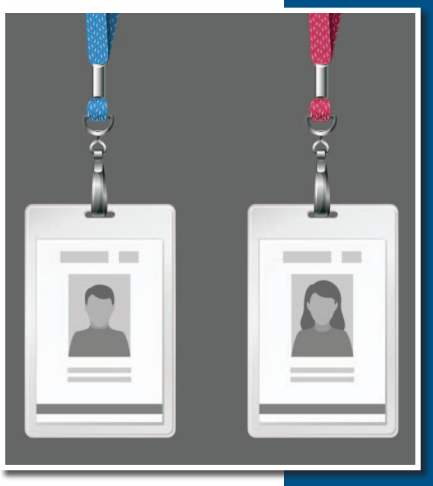
In the event of a credible threat to your venue, geographic area, or industry:

- Escort all delivery vehicles to the area within the venue where the delivery is made.
- Tow illegally parked vehicles.
- Reduce the number of access points for pedestrians and vehicles. Increase the security (additional guards and inspections) at each open access point.
- Restrict access by non employees (contractors, vendors, visitors) to those needed to support critical activities. Delay non-essential contractor work. Escort essential vendors and contractors while on the premises.
- Review available threat information and consult with law enforcement authorities to determine if the venue should be closed.

4.5 Credentialing

Credentialing procedures offer the means to identify key personnel within a venue, as well as control access. Credentialing options may range from electronic badges used in year-round fixed venues to colored shirts and hats worn by volunteers at a community gathering. Consider the following credentialing measures:

- Devise credential systems that indicate.
  - Areas of access (e.g., utility and mechanical areas, entertainment stage, viewing stand for a parade, livestock areas for state fair).
  - Purpose of activity on the premises (e.g., concessions, operations, security).



- Consider color-coding the credentials for easier identification.
- Issue photo identification badges to all employees.
- For venues with fixed gates and fences, consider requiring that employees swipe badges before entering the premises.
- Use colored shirts, jackets with emblems, hats, and badges so that personnel with special functions are identifiable not only to the public but to other personnel working at the venue. Key personnel such as a security person with a radio) should be easily identifiable to others working at the venue. This is particularly important when there are volunteers or temporary employees staffing the event, because they may not be as familiar with other personnel as full-time employees.
- 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, vendors, and volunteers wear credentials issued by venue 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 venue. Individuals who do not return credentials should be identified and those credentials should be deactivated.

4.6 Signage and Notification

Signage and notification are essential to convey important information to guests visiting outdoor venues. The signage protective measures described below should be considered for use by outdoor venues:

- Publicize rules and basic visitor information ahead of time. Provide information on venue entrances, prohibited items, location of parking areas, and public transportation routes accessible to the venue. In addition, publicize whether hand carried items such as purses and backpacks) are subject to inspection. Make this information available on the venue's Web site, in radio announcements, on tickets, and in newspaper advertisements so that attendees can plan their visit and are not surprised when items such as coolers or backpacks are not allowed at the venue.
- Ensure signage in parking areas identifies items (e.g., backpacks, glass containers, coolers) that visitors may not carry into the venue.
- Ensure signage clearly marks what types of access is allowed through a particular area of the venue. Signage is also recommended for directing delivery trucks to their appropriate destination and checkpoint.
- 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.
- Establish a "Security Awareness Campaign" through information provided on the venue's Web site, mailings, and signage on the grounds to encourage patrons and workers to report suspicious activity to the nearest venue staff, security officer, or law enforcement officer.

4.7 Barriers

The use of physical barriers and controls can serve a variety of purposes at an outdoor venue. 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). In open areas adjacent to roadways, barriers are critical to protecting crowds from vehicular traffic.

Venue Perimeter Barriers

- Evaluate the need for perimeter barriers around the venue. Consider natural features such as hills, woods, waterways that could either enhance or inhibit security at the facility. For outdoor events in an open area, consider temporary railings and fences.

- Implement appropriate level of barrier security at fixed venues (e.g., chain-link fencing, chained gates, 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.

Building Barriers

- Establish clear zones adjacent to sensitive or critical buildings. Keep zone free of obstructions to allow for continuous monitoring and to inhibit concealment of people or packages.
- If appropriate, install building perimeter barriers (e.g., fences, bollards, decorative flowerpots, high curbs) 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 chemical, biological, or radiological agents from being introduced into any buildings on the premises.
- Move objects that could become projectiles (e.g., trash containers, crates, 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.

Vehicle Barriers

- Evaluate vehicle traffic patterns around and within the venue. 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 vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from buildings and areas where people congregate. *FEMA 430: Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*[4] provides information and design concepts for the protection of buildings and occupants. Chapters on *Perimeter Security Design* and *Security Design for the Open Site* have information on the effectiveness of vehicle barriers. (See Appendix D: Additional Resources – Web Sites).
- Install removable bollards on pedestrian walkways to keep unauthorized vehicles off walkways.

[4] FEMA, Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks, www.fema.gov/library/viewRecord.do?id=3135, accessed February 21, 2011.

In the event of a credible threat to your venue, geographic area, or industry:

- Deploy temporary barriers (e.g., bollards, Jersey barriers, heavy vehicles, and equipment) to increase standoff distances and provide additional access control.
- Deploy temporary barriers to slow the flow of traffic into the venue.

4.8 Communication and Notification

Communication protective measures for an outdoor venue 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 an emergency.

Communications Equipment

- Ensure there are systems (e.g., public address, cell phones, pagers, etc.) that provide a timely means to communicate with all people at the venue including employees, security personnel, emergency response teams, and patrons in order to notify and instruct what to do in an emergency situation. There must be reliable, secure communications such as handheld two-way radios between the emergency operations center and the employees operating the public address system and video screens in order for the emergency command center to authorize and direct the broadcast of emergency scripts and messages.
- Provide redundant communication channels (e.g., telephone, radio, pager, public address system) that can be used in the event that one channel is disabled.
- Ensure that there are procedures and equipment for communicating with local law enforcement and emergency responders. Test systems regularly and train employees in the use of the communication systems.
- Have emergency communication equipment such as special cell phones, emergency radios) available for use in the event that all primary channels are unavailable.
- 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 notification protocol that outlines who should be contacted in emergencies. Designate who is to contact whom within the venue and within 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 the current 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 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.

Information Sharing

- Monitor industry and government information on threats, incidents, and response procedures. Report information about the venue's experiences with suspicious or criminal activity to the nearest State and local fusion center and to the local FBI Joint Terrorism Task Force. The nearest State and local fusion center's contact information can be found on the Homeland Security Information Network-Critical Sectors (HSIN-CS). (To register for HSIN-CS, e-mail: hsin.help.desk@dhs.gov). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact-us/field. (See Appendix C: Additional Federal Resources for more information on fusion centers and FBI Joint Terrorism Task Forces).

In the event of a credible threat to your venue, geographic area, or industry:

- Increase frequency of communications with local law enforcement. Advise them of the heightened security status at the venue. 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.
- Increase the frequency of reporting and call-ins from employees, particularly those in remote areas of the venue.
- Test communication equipment, including primary and backup systems frequently. Have backup communication equipment activated and ready for use.

4.9 Monitoring, Surveillance, 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 outdoor venue operations and security requirements. Begin monitoring operations at a standoff distance and continuing monitoring closer to the center of activity. Coordinate with local law enforcement on activities to be undertaken, particularly with regard to monitoring activities in the area surrounding venue.

- Monitor work being done adjacent to the venue (e.g., road construction, utility equipment servicing) for signs of unusual activities (e.g., planting packages near assets or gathering places).
- Ensure security personnel regularly inspect the site perimeter, parking lots, equipment, trash containers, and sensitive or critical areas for signs of security issues. Even if there are roving patrols of the venue, individuals may need to be assigned to stages or other special areas where there is equipment to prevent theft or tampering.
- Train security staff to identify surveillance techniques including identifying 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.

- Assess the need for surveillance cameras to provide coverage for the perimeter, sensitive and critical areas, vehicle roadways, parking lots, and the buffer zone around the venue. Consider video surveillance equipment (e.g., closed-circuit television(CCTV), lighting). Provide coverage for the perimeter, sensitive and critical assets in the venue, vehicle roadways and parking lots, and building entrances. Include coverage of buffer zone around the venue.
- If surveillance cameras are used, train personnel to interpret video and identify potential security-related events. Review recordings regularly for unusual activities or patterns. If appropriate, provide video feed to local law enforcement. Inspect and test all video equipment regularly.
- Mount digital security cameras on high structures within the venue. These can be used to assist security on the ground in finding a customer who is trying to avoid security or to find a lost child.
- Monitor people entering and leaving the venue. Train monitors to detect 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 facility for unusual behavior.
- Inspect packages and backpacks carried by people entering sensitive or critical areas, including employees, vendors, and visitors.

Vehicles

- Monitor all vehicles approaching an entrance or gathering of people for signs of threatening or suspicious behavior (e.g., unusually high speed, vehicles riding particularly low, vehicles emitting a chemical odor, occupants keeping the windows open even in cold or inclement weather). Prepare to take defensive action against vehicles exhibiting such behavior (e.g., engage barriers, deploy security vehicles).
- Use random inspections or inspection of all vehicles, as appropriate.

Deliveries and Mail

- Supervise the unloading of materials and equipment. 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 procedures: Inspect all mail for unusual signs such as leaking powders, strange odors, 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. (See Appendix A: Suspicious Mail or Packages).
- Maintain records of all deliveries.

In the event of a credible threat to your venue, geographic area, or industry:

- Increase monitoring and surveillance of sensitive and critical assets, people, vehicles, materials, and equipment. Reassign personnel to assist in surveillance monitoring and inspections.
- Increase monitoring of video surveillance, alarms, and equipment detectors.
- Install additional temporary lighting to provide increased illumination.
- Thoroughly inspect all vehicles and deliveries made to the venue.
- Consider processing deliveries at a remote site.

4.10 Information Security and Cybersecurity

Information kept on venue computers – customer, company, and financial information – is crucial to business operations and if lost, damaged, or stolen, may impact security. As infiltration via cyber networks has the potential to shut down day-to-day operations and exploit, corporate, personal, or financial information, consider these measures to assist in protecting information and vital computer systems:

- Develop and implement a security plan for computer and information systems, hardware and software associated with the venue. Design and implement secure computer network architecture and ensure that business and enterprise security policy is followed.

- Install and maintain up-to-date cybersecurity techniques (e.g., firewalls, virus protection, spyware protection encryption, user authentication) and software patches. Monitor computer systems regularly to detect any patterns of probing, hacking, or intrusions.
- Regularly test computer security measures such as audits and penetration testing.
- Identify any critical communications, industrial control (such as access control, HVAC, water distribution systems), and information technology systems that support critical venue operations and implement cybersecurity defensive technologies to protect them from unauthorized access.
- Control physical access to IT equipment (e.g., computer rooms, payment systems, surveillance systems, and areas where control systems that operate rides and other operations are housed). Install locks and access controls to allow only authorized personnel to enter. Provide communication capabilities to allow rapid reporting of incidents.
- Ensure that vendors practice up-to-date cybersecurity techniques (e.g., firewalls, user authentication). Monitor control and payment systems regularly to detect patterns of hacking or intrusion.
- 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.
- Develop a recovery and restoration plan to return computer and control systems to full functionality after an incident. Test these plans and procedures.
- Test all applications that involve the handling of sensitive information for potential vulnerability to compromise.
- Review the venue's Web site to ensure it does not contain any sensitive information such as staff contact information, proprietary information, financial information, host or customers details, technical specifications, and chemical and biological data. Ensure that the Web site is protected with up-to-date security software.

4.11 Infrastructure Interdependencies

Theme parks, amusement parks, and fairgrounds are complex entities that must rely on utilities and other infrastructure to continue their day-to-day operations. For outdoor gatherings that occur only once or a few times a year, infrastructure to support the event may have to be put in place especially for the event (e.g., portable toilets, generators). 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 outdoor venue.

- ❍ Establish regular communication channels with utility service providers identified above 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.

- ❍ Determine 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)

- ❍ Where practical, provide for redundancy and emergency backup capability for critical support architectures. Where possible, locate the redundant and backup equipment in a different part of the venue than where the primary supply equipment is located. Inspect and maintain backup equipment regularly.
- ❍ Locate movable utility supplies that are potentially hazardous such as liquid fuel tanks and chlorine tanks in secure areas a safe distance from buildings and areas where large numbers of people congregate. If possible, locate these supplies off site. Monitor the safeguarding of any products and/or chemicals that must be stored on site, and handle in compliance with State regulations.
- ❍ Ensure that liquefied petroleum gas (LPG) used for outdoor catering operations is not accessible to the crowd and is protected from the threat of theft.
- ❍ Notify the fire department of the location of large quantities of LPG, diesel fuel, or gasoline on the premises.
- ❍ 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.

In the event of a credible threat to your venue, geographic area, or industry:

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

4.12 Food and Beverage Services

Outdoor venues incorporate a wide range of food and beverage services, including restaurants and open air concession stands. In some cases, food may be the central theme of a festival. Consider the following measures for food service operations:

Planning

- Coordinate with the local health department to assess food security procedures and operations. For outdoor gatherings that take place only once or a few times a year, coordinate with the health department during the planning stage. The U.S. Department of Health and Human Services Food and Drug Administration's (FDA) *Guidance for Industry: Retail Food Stores and Food Service Establishments: Food Security Preventive Measures Guidance*[5] is a resource for planning and implementing food security measures.
- Ensure that all food service operations, including those of concessionaires, have the appropriate permits and licenses.
- Install portable hand-washing stations.

Training

- Incorporate food security awareness into staff training, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats. Include temporary, contract, and volunteer staff in training. Ensure that concessionaires are trained in methods to prevent and identify food contamination and that they meet all required certifications. The FDA's *Employee's FIRST*[6], is an FDA initiative that food industry managers can include in their ongoing food defense training programs. (*See Appendix D: Additional Resources – Web Sites*).

Incoming Products

- Use only known and appropriately licensed or permitted sources for incoming products, where applicable.
- Inform suppliers, distributors, and transporters about FDA's Guidance for Industry: *Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance*[7].
- Establish food and beverage delivery schedules. Do not accept unexplained or unscheduled deliveries (see section 4.9). Investigate delayed or missed shipments.
- Record food and beverage deliveries with the date, time, vehicle registration number, and company name; obtain identification information from the person(s) making deliveries.

---

[5] US Food and Drug Administration, www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/GuidanceDocuments/FoodDefenseandEmergencyResponse/ucm082751.htm, accessed February 21, 2011.

[6] U.S. Food and Drug Administration, www.fda.gov/Food/FoodDefense/Training/ucm135038.htm, accessed February 21, 2011.

[7] U.S. Food and Drug Administration, www.fda.gov/Food/FoodDefense/FoodSecurity/default.htm.

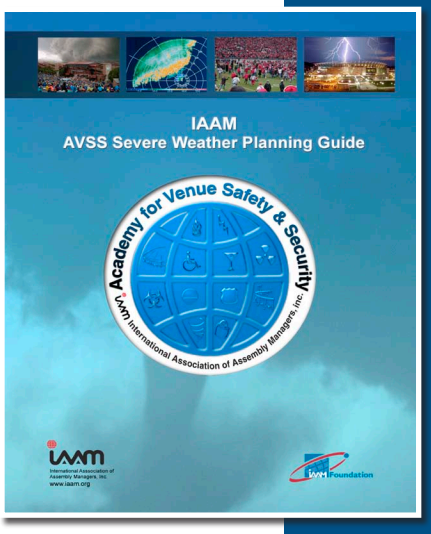
- Supervise off-loading and inspect incoming products for signs of tampering, contamination, or damage (e.g., abnormal stains or odors, evidence of resealing) or counterfeiting (e.g., inappropriate or mismatched product identity and labeling, absence of tamper-evident packaging when the label contains a tamper-evident notice).
- Reject the delivery of suspect food and notify food distributors and local law enforcement of actual or suspected tampering incidents.
- Ensure that refrigerated trucks and other trucks and containers used to store food on the premises are locked.

Monitoring and Inspection

- Perform random food security inspections of all appropriate areas of the venue including receiving and warehousing, where applicable.
- Ensure that "Use By" dates are still valid.
- Monitor the serving or display of foods in self-service areas (e.g., condiment stations and salad bars).

4.13 Special Considerations – Hazardous Weather

Hazardous weather presents a special challenge to outdoor venues. Patrons are typically spread out over a large area and there are few, if any, facilities available for shelter. Of particular concern are severe weather events such as tornados, hail, high winds, and lightning that may occur with limited advance warning. Hazardous weather preparedness is necessary to protect the safety of visitors and personnel, as well as assets of the venue.



- Develop a hazardous weather preparedness plan as part of the venue's Emergency Response Plan. The International Association of Venue Managers' (IAVM) *Severe Weather Planning Guide*[8] is a resource that provides public assembly venue managers with a basic understanding of severe/hazardous weather events and how to establish a plan for what to do in advance of, during, and after such situations and is available for purchase from IAVM.

- Consider the following in the development of a hazardous weather preparedness plan:
  - Assess the threats to the outdoor venue and the strengths and weaknesses of the venue's infrastructure and available resources.
  - Identify who is charge of the severe weather preparedness and who is authorized to make the decision to evacuate, shelter in place, or relocate.
  - Coordinate the plan with local emergency authorities.

[8] IAVM, Severe Weather Planning Guide, *www.iavm.org/Shop/List.asp?CatID=2*, accessed February 21, 2011.

- Coordinate with the National Weather Service to stay up-to-date with natural hazard conditions that could adversely impact operations or force a shut down or evacuation of the venue. The FEMA Emergency Management Institute Course, "*Anticipating Hazardous Weather & Community Risk* (IS-271),[9]" provides guidance to emergency managers to anticipate and prepare for hazardous weather through familiarization with NWS products and development of partnerships with the NWS in advance of any threat. IAVM offers a specialized training class and a Webinar on severe weather planning. Information is available on the IAVM Web site.[10]
- If the venue uses a National Oceanic and Atmospheric Administration (NOAA) radio or lightning detection equipment/software, ensure that personnel have the appropriate training and are monitoring it for hazardous weather conditions.
- Consider working with a private weather company to provide fee-for-forecast services, including e-mail, and pager notification.
- Evaluate the need for lightning detection equipment.
- Evaluate the need for sirens.
- Post instructions on the venue's Web site, on placards in the parking area, and within the venue explaining what to do in the event of lightning or other severe weather.

---

[9] FEMA Emergency Management Institute, IS-271 Anticipating Hazardous Weather & Community Risk, http://training.fema.gov/EMIWeb/IS/is271.asp, accessed February 21, 2011.

[10] IAVM Web page, www.iavm.org/, accessed February 21, 2011.

List of Acronyms and Abbreviations

ASIS	American Society for Industrial Security
CBR	Chemical Biologocal Radiological
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control and Prevention
CSVA	Cybersecurity Vulnerability Assessment
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
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network – Critical Sectors
HVAC	Heating Ventilating and Air Conditioning
IAVM	International Association for Venue Managers
ID	Identification
IED	Improvised Explosive Device
IT	Information Technology
LPG	Liquefied Petroleum Gas

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
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. In the Incident Command System, agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance). Governmental organizations are most often in charge of an incident, though in certain circumstances private-sector organizations may be included. Additionally, nongovernmental organizations may be included to provide support.[4]

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

Asset. 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 on 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.

- 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

---

1 U.S. Department of Homeland Security, Federal Emergency Management Agency. The National Incident Management System (NIMS), http://www.fema.gov/emergency/nims, accessed February 22, 2011.

2 U.S. Department of Homeland Security, Active Shooter: How to Respond, http://www.alerts.si.edu/docs/DHS_ActiveShooterBook.pdf?bcsi_scan_24F6D4EFE9292259=GAuFFt5Ei3p0NCJAODWiMTM9g2wlAAAAoM+qoQ==&bcsi_scan_filename=DHS_ActiveShooterBook.pdf, accessed February 22 2011.

3 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

4 U.S. Department of Homeland Security, National Response Framework, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed February 22, 2011.

5 The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/PotentialTerroristAttackMethods.pdf, accessed February 22, 2011.

6 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

7 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

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.[8]

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 that do not make those individuals contagious to others (e.g., anthrax, botulinum toxin).[9]

Bomb Threat. The communication through the use of mail, e-mail, 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. Spreading of chemicals with the intent to do harm. The Chemical Weapons Convention defines a chemical weapon as "any toxic chemical or its precursor that can cause death, injury, temporary incapacitation, or sensory irritation through its chemical action."[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 making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files. Viruses used to be spread when people shared floppy disks and other portable media. Now viruses are primarily spread through email messages.[13]

Consequence. Effect of an event, incident, or occurrence.[14]

Countermeasure. Action, measure, or device that reduces an identified risk.[15]

---

8 U.S. Department of Transportation, Transit Security Design Considerations, http://www.globalsecurity.org/security/library/report/2004/transit-security-design_appd.htm, accessed February 2011.

9 U.S. Department of Homeland Security. Biological Attack: What Is It?, http://www.dhs.gov/files/publications/gc_1245181954420.shtm, accessed February 22, 2011.

10 University of Tennessee-Martin. Bomb Threat Information, http://www.utm.edu/alerts/bomb.php, accessed February 22, 2011.

11 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

12 The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/PotentialTerroristAttackMethods.pdf, Accessed February 22, 2011.

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 February 22, 2011.

14 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

15 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

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.[16]

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.[17]

Cybersecurity Vulnerability Assessment (CSVA). A process that draws on an automated set of questions to assess an entity's cyber security posture and recommend a suite of remedial actions to address any observed security gaps. The methodology will assess an organization, facility, or system's cyber vulnerabilities and provide explanations, examples, and options for consideration when potential cyber security enhancements could be implemented.[18]

Cybersecurity. All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures. Cyber-security risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability or conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.[19]

Deterrent. Measure that discourages an action or prevents an occurrence by instilling fear, doubt, or anxiety.[20]

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.[21]

Emergency Management. A subset of incident management consists of the coordination and integration of all activities necessary to build, sustain, and improve the capability to prepare for,

---

16 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

17 U.S. Department of Defense, Cyberspace Glossary, *http://www.pcmag.com/encyclopedia_term/0,2542,t=DOD+cyberspace+glossary&i=62535,00.asp*, accessed February 2, 2011.

18 U.S. Department of Homeland Security, Federal Emergency Management Agency, Homeland Security Grant Program – Cyber Security Guidance, *http://www.bhs.idaho.gov/Pages/FinanceAndLogistics/Grants/PDF/fy08_hsgp_guide_cyber.pdf*, accessed February 22, 2011.

19 U.S. Department of Defense, Cyberspace Glossary, *http://www.pcmag.com/encyclopedia_term/0,2542,t=DOD+cyberspace+glossary&i=62535,00.asp*, accessed February 2, 2011.

20 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

21 U.S. Department of Homeland Security, Federal Emergency Management Agency. The National Incident Management System (NIMS), *http://www.fema.gov/emergency/nims*, accessed February 22, 2011.

protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other manmade disasters.[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 Plan. The ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.[24]

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

Function. 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. Natural or manmade source or cause of harm or difficulty.[28]

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.[29]

Implementation. Act of putting a procedure or course of action into effect to support goals or achieve objectives.[30]

Improvised Explosive Device (IED). A homemade bomb and/or destructive device used to destroy, incapacitate, harass,

---

22 U.S. Department of Homeland Security, Federal Emergency Management Agency. The National Incident Management System (NIMS), http://www.fema.gov/emergency/nims, accessed February 22, 2011.

23 U.S. Department of Homeland Security, Federal Emergency Management Agency. The National Incident Management System (NIMS), http://www.fema.gov/emergency/nims, accessed February 22, 2011.

24 U.S. Department of Homeland Security, Federal Emergency Management Agency, National Response Framework Center, http://www.fema.gov/emergency/nrf/glossary.htm#E, accessed February 22, 2011.

25 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

26 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

27 U.S. Department of Homeland Security. State and Local Fusion Centers, http://www.dhs.gov/files/programs/gc_1156877184684.shtm, accessed February 22, 2011.

28 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

29 U.S. Department of Homeland Security, Homeland Security Information Network, http://www.dhs.gov/files/programs/gc_1156888108137.shtm, accessed February 22, 2011.

30 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

or distract. IEDs are used by criminals, vandals, terrorists, suicide bombers, and insurgents.[31]

Incident. Occurrence, caused by either human action or natural phenomena that may cause harm and that may require action.[32]

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.[33]

Intent. A state of mind or desire to achieve an objective.[34]

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.[35]

Key Resources. As defined in the Homeland Security Act, key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.[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).

Malicious Code. Any software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.[37]

Manmade Hazards. Typically associated with a criminal or terrorist attack using a weapon such as an explosive, biological, or chemical agent.[38]

Maritime Attack. This attack method involves using maritime vessel toundertake terrorist acts and activities within the maritime environment.[39]

---

31 U.S. Department of Homeland Security, Improvised Explosive Device Fact Sheet, http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, accessed February 22, 2011.

32 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

33 U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed February 22, 2011.

34 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

35 U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed February 22, 2011.

36 U.S. Department of Homeland Security, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed February 22, 2011.

37 National Security Agency, Guidance for Addressing Malicious Code, http://www.nsa.gov/ia/_files/Guidance_For_Addressing_Malicious_Code_Risk.pdf, accessed February 22, 2011.

38 U.S. Department of Homeland Security, Office of the Inspector General, FEMA's Progress in All Hazards Mitigation, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-03_Oct09.pdf, accessed February 22, 2011.

39 The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/PotentialTerroristAttackMethods.pdf, accessed February 22, 2011.

Mitigation. Ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident.[40]

Natural Hazard. Source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena.[41]

Network. Group of components that share information or interact with each other in order to perform a function.[42]

Nuclear or Radiological Attack. An attack method using a weapon with explosive power resulting from the release of energy by the splitting of nuclei of a heavy chemical element, such as plutonium or uranium (fission), or by fusing of nuclei from a light element, such as hydrogen (fusion).[43]

Physical Security. Describes measures used to protect assets (including computers) from damage caused by physical forces such as explosion, impact and fire.[44]

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.[45]

Protective Measures. Includes 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.

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 terrorists; that is, make the facility less interesting as a target.[46]

Resilience. Ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.[47]

Risk. Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.[48]

Risk Assessment. Explicit or implicit decision not to take an action that would affect all or part of a particular risk.[49]

---

40 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

41 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

42 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

43 The Federal Bureau of Investigation (FBI), Potential Terrorist Attack Methods, http://info.publicintelligence.net/PotentialTerroristAttackMethods.pdf, accessed February 22, 2011.

44 Congressional Research Service (CRS), Critical Infrastructure and Key Resources: Definition and Identification, http://www.fas.org/sgp/crs/RL32631.pdf, accessed February 22, 2011.

45 U.S. Department of Homeland Security, Federal Emergency Management Agency, NIMS Resource Center: Glossary of Terms, http://www.fema.gov/emergency/nrf/glossary.htm, accessed February 22, 2011.

46 Homeland Security Institute, Homeland Security Strategic Analysis: Mission Area Analysis, http://www.homelandsecurity.org/hsireports/MAAReportFinal28Mar07public.pdf, accessed February 22, 2011.

47 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

48 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

49 U.S. Department of Homeland Security, Risk Lexicon, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed February 22, 2011.

Risk Management. Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost and benefits of any action taken.[50]

Risk Mitigation. Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.[51]

Scenario (Risk). Hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate.[52]

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 18 Critical Infrastructure sectors.[53]

Security Awareness. The knowledge and attitude members of an organization possess regarding the protection of the physical and, especially, information assets of that organization.[54]

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 attacker. Some spyware can even allow the attacker to control the infected computer remotely.[55]

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.[56]

Target. Asset, network, system, or geographic area chosen by an adversary to be impacted by an attack.[57]

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. Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.[58]

---

50 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

51 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

52 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

53 U.S. Department of Homeland Security, National Infrastructure Protection Plan, *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf*, accessed February 22, 2011.

54 Rutgers University, Security, Awareness, Training and Communication, *http://rusecure.rutgers.edu/content/security-awareness-training-and-communication*, accessed February 22, 2011.

55 U.S. Department of Homeland Security, Computer Emergency Readiness Team (US-CERT), Spyware, *http://www.us-cert.gov/reading_room/spywarehome_0905.pdf*, accessed February 22, 2011.

56 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

57 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

58 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

Threat Assessment. 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.[59]

TRIPwire Community Gateway. 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.[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 e-mail messages.[61]

Vehicle-borne IEDs (VBIED). Vehicular-borne improvised explosive devices laden with explosives and driven directly at a target.[62]

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

---

59 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

60 U.S. Department of Homeland Security, Technical Resources for Incident Prevention (TRIPwire), *http://www.dhs.gov/files/programs/gc_1184339971040.shtm*, accessed February 22, 2011.

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 February 22, 2011.

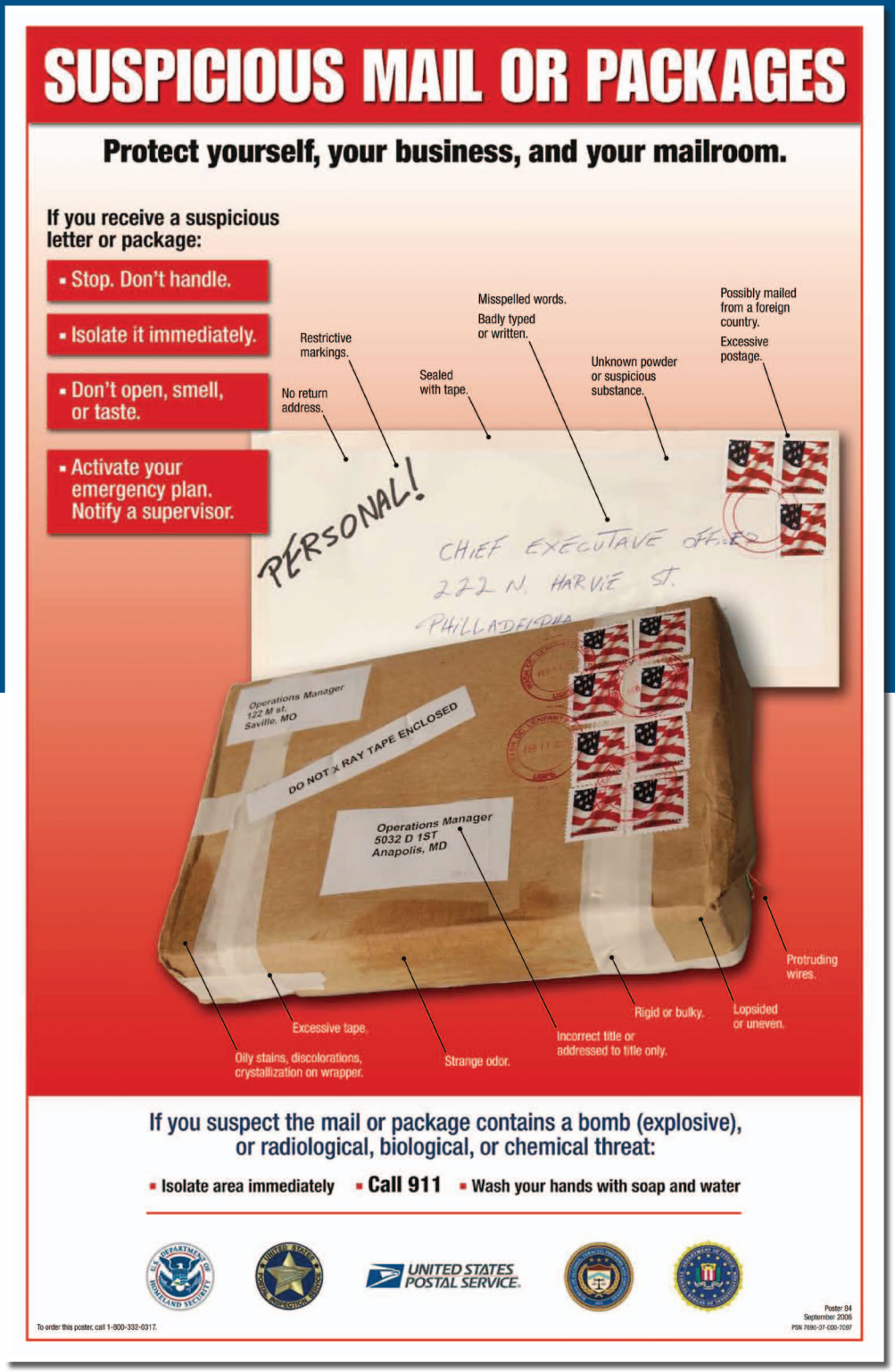
62 Congressional Research Service (CRS), Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures, *http://research.fit.edu/fip/documents/SecNews1.pdf*, accessed February 22, 2011.

63 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

64 U.S. Department of Homeland Security, Risk Lexicon, *http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf*, accessed February 22, 2011.

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 February 22, 2011.

Appendix A: Suspicious Mail or Packages



U.S. Postal Service Suspicious Mail or Packages Poster
www.usps.com/communications/news/security/suspiciousmail.htm

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 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
- Activate your emergency plan
- Notify a supervisor

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 e-mail:

- 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

Other Information:

_____

_____

Threat Language:

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

_____

_____

_____

Homeland Security

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

Appendix C: Additional Federal Resources

Homeland Security Information Network (HSIN)

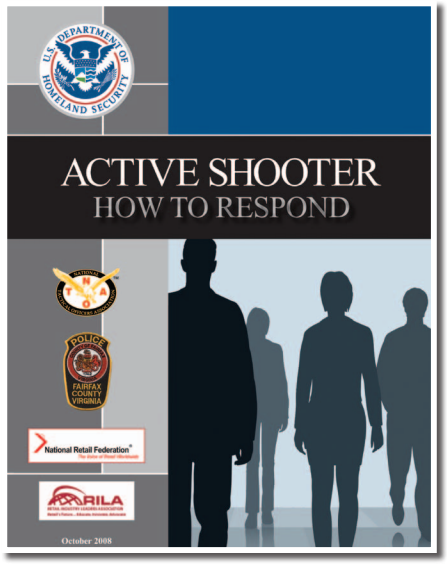
HSIN is an Internet-based platform used by the U.S. Department of Homeland Security (DHS) to facilitate the sharing of information necessary for coordination, operational plans, mitigation, and response to incidents by the government and the private sector.

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 Outdoor Venues 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 the U.S. Outdoor Venues Industry*
- "HSIN Jabber" instant messaging tool
- Web conferencing
- Incident reporting
- Common Operational Picture (COP), which provides situational awareness and analysis
- Integrated Common Analytical Viewer (iCAV), which gives geographical visualization
- 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 e-mail address, phone number, organization, job title/responsibilities, supervisor's name, supervisor's e-mail address, phone number, and note that you are part of the Outdoor Venues Subsector.

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

To determine which information-sharing environment most meets your needs, please go to http://www.dhs.gov/files/programs/gc_1189168948944.shtm and click on the appropriate box to receive specific critical information sector information.

Training and other resources highlighted in HSIN include:

- Soft Target Awareness Course
- Protective Measures Course
- Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff Course
- Bomb-Making Materials Awareness Program
- What's in Store: Ordinary People/ Extraordinary Events video
- No Reservations: Suspicious Behavior in Hotels video

TRIPwire Community Gateway

TRIPwire Community Gateway is 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 18 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 Sectors (HSIN-CS) 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 decision-making 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.[66]

Protective Security Advisors: Providing Community-Based Support

Established in 2004, the Protective Security Advisor (PSA) Program provides a DHS security expert as the link between State, local, tribal, and territorial organizations

[66] US DHS, National Network of Fusion Centers Fact Sheet, *www.dhs.gov/files/programs/gc_1296484657738.shtm*, accessed February 21, 2011.

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 provide a local perspective to the national risk picture.

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; and
- 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: psadutydesk@hq.dhs.gov.

Vulnerability Assessments

The DHS conducts specialized facility assessments to identify vulnerabilities of critical infrastructure, including assets within the Commercial Facilities Sector and Outdoor Venues 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 Cyber Security Evaluation Tool (CSET)

DHS 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 (NCSD) 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 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.

Appendix D: Additional Resources–Web Sites

U.S. Department of Homeland Security's Protecting Critical Infrastructure Web site

Protecting and ensuring the continuity of the critical infrastructure of the United States are essential to the 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.
- *What's in Store: Ordinary People | Extraordinary Events*. A video 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: www.dhs.gov/cfsector.

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. www.us-cert.gov/reading_room/distributable.html

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

Ready.gov is a national campaign designed to educate and empower Americans to prepare for and respond to emergencies, including natural disasters and potential terrorist attacks. The goal of the campaign is to get the public involved and ultimately to increase the level of basic preparedness across the nation. www.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.
www.ready.gov/business/index.html

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

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, 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.
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.
www.us-cert.gov

American Association of Poison Control Centers (AAPCC)

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.
www.aapcc.org/DNN/

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.
www.asisonline.org/

ASIS International's 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.
www.asisonline.org/guidelines/published.htm

Canadian Center for Emergency Preparedness

The Canadian Centre for Emergency Preparedness (CCEP) is a federally incorporated, not-for-profit organization based in Burlington, Ontario. Its goal is to foster the development of a disaster-resilient Canada through individuals, communities, and businesses.
http://www.ccep.ca/

Centers for Disease Control and Prevention (CDC)

CDC serves as the national focus for developing and applying disease prevention and control, environmental health, and 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. 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/

Centre for the Protection of National Infrastructure

The United Kingdom's Centre for the Protection of National Infrastructure (CPNI) provides integrated security advice (combining information, personnel, and physical) to the businesses and organizations which make up the national infrastructure. Through the delivery of this advice, CPNI protects national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats. www.cpni.gov.uk/

Centre for the Protection of National Infrastructure – Good Practice Guide on Pre-Employment Screening

CPNI's Pre-Employment Screening is the latest in a series of advice products on the subject of personnel security. It provides detailed guidance on pre-employment screening measures including identity checking, confirmation of the right to work in the UK, and verification of a candidate's historical personal data (including criminal record checks). http://www.cpni.gov.uk/documents/publications/2009/2009024-gpg_pre_employment_screening.pdf

Centre for the Protection of National Infrastructure – Ongoing Personnel Security: A Good Practice Guide

The guidance provides information about good practice in ongoing personnel security, bringing together advice from government departments and private organizations in a single document focusing on the key elements of an effective security culture. http://www.cpni.gov.uk/documents/publications/2010/2010021-gpg_ongoing_personnel_security.pdf

Centre for the Protection of National Infrastructure – Protecting Against Terrorism (3rd Edition)

This 38-page booklet gives general protective security advice from CPNI. It is aimed at businesses and other organizations seeking to reduce the risk of a terrorist attack, or to limit the damage terrorism might cause. http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf

Centre for the Protection of National Infrastructure – Risk Assessment for Personnel Security

This personnel security assessment focuses on employees, their access to the organization's assets, the risks they could pose to the organization, and the sufficiency of countermeasures. It is the foundation of the personnel security-management process. It is also

crucial in helping security and human resource managers communicate to senior managers the risk to which the organization is exposed. http://www.cpni.gov.uk/documents/publications/2010/2010037-risk_assment_ed3.pdf

Centre for the Protection of National Infrastructure - Guide to Producing Operational Requirements for Security Measures

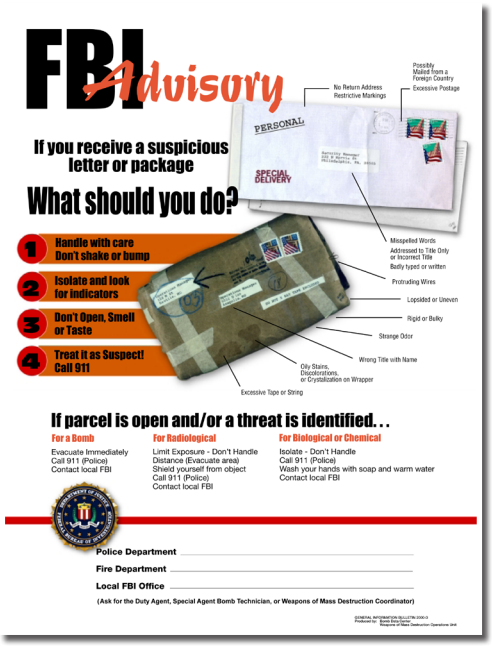
This guide aimed at ensuring that appropriate security measures are recommended to manage the risk to a level acceptable to all stakeholders. It introduces the concept of a structured methodology for determining the security requirements. http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf

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/

Federal Bureau of Investigation (FBI)

This PDF presentation from the FBI 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



Federal Emergency Management Agency (FEMA)

FEMA has nearly 4,000 standby disaster assistance employees who are available for deployment after disasters. www.fema.gov/

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/

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

- *Active Shooter, What You Can Do* (IS-907) – A training course developed to provide 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
- *Workplace Security Awareness* (IS-906) - This course provides guidance to individuals and organizations on how to improve the security in your workplace. http://training.fema.gov/EMIWeb/IS/is906.asp

FEMA Security Risk Management Series (RMS) Publications

The Risk Management Series (RMS) is a FEMA series directed at providing design guidance for mitigating multi-hazard events. The series includes a large cadre of manmade disaster publications directed at strengthening 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. www.fema.gov/plan/prevent/rms/

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

Part of the FEMA's Security Risk Management Series, this manual provides guidance to the building science community of architects and engineers to reduce physical damage caused by terrorist assaults to buildings, related infrastructure, and people. The manual presents incremental approaches that can be implemented over time to decrease the vulnerability of buildings to terrorist threats. Many of the recommendations can be implemented quickly and cost effectively.
www.fema.gov/plan/prevent/rms/rmsp426

FEMA 430: Site and Urban Design for Security: Guidance against Potential Terrorist Attacks

Part of the FEMA's Security Risk Management Series, this training provides information and design concepts for the protection of buildings and occupants, from site perimeters to the faces of buildings. The intended audience includes the design community of architects, landscape architects, engineers, and other consultants working for private institutions, building owners and managers, and State and local government officials concerned with site planning and design.
www.fema.gov/library/viewRecord.do?id=3135

FEMA 452: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks

Part of the FEMA's Security Risk Management Series, the objective of this how-to guide is to outline 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 scope of the methods includes reducing physical damage to structural and nonstructural components of buildings and related infrastructure, and reducing resultant casualties during conventional bomb attacks, as well as attacks involving CBR agents.
www.fema.gov/plan/prevent/rms/rmsp452.shtm

FEMA 453: Safe Rooms and Shelters - Protecting People Against Terrorist Attacks

Part of the FEMA's Security Risk Management Series, the objective of this manual is to provide guidance for engineers, architects, building officials, and property owners to design shelters and safe rooms in buildings. This manual presents information about the design and construction of shelters in the workplace, home, or community building that will provide protection in response to manmade hazards.
www.fema.gov/library/viewRecord.do?id=1910

FEMA 455: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks

Part of the FEMA's Security Risk Management Series, this manual provides guidance for building inspectors, architects and engineers on quickly and effectively determining what, if any, are the risks posed to the building by natural hazards, terrorist attacks, and other threats to the building's structural integrity.
www.fema.gov/library/viewRecord.do?id=1567

FEMA 459: Incremental Protection for Existing Commercial Buildings from Terrorist Attack

Part of the FEMA's Security Risk Management Series, this manual provides guidance to owners of existing commercial buildings and their architects and engineers on security and operational enhancements to address vulnerabilities to explosive blasts and CBR hazards. It also addresses how to integrate these enhancements into the ongoing building maintenance and capital improvement programs. These enhancements are intended to mitigate or eliminate long term risk to people and property.
www.fema.gov/library/viewRecord.do?id=3270

Federal Emergency Management Agency – 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 (RVS) 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.
www.fema.gov/library/viewRecord.do?id=3556

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

OSHA's mission is to prevent work-related injuries, illnesses, and deaths by issuing and enforcing rules (called standards) for workplace safety and health. www.osha.gov

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 (bird), and pandemic influenza for the general public, health, and emergency preparedness professionals, policy makers, government and business leaders, school systems, and local communities. www.flu.gov/

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. www.infragard.net/

National Emergency Management Association (NEMA)

NEMA is the professional association of and for emergency management directors from all 50 states, eight territories, and the District of Columbia. The primary purpose of NEMA is to be the source of information, support, and expertise for emergency management professionals at all levels of government and the private sector who prepare for, mitigate, respond to, recover from, and provide products and services for all emergencies, disasters, and threats to the Nation's security. http://www.nemaweb.org/

National Fire Protection Association (NFPA)

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. 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 NOAA provides weather and climate forecasts and warnings for the U.S. This is done through a collection of national regional centers and more than 120 local weather forecast offices. 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. www.nws.noaa.gov/

Office for Security and Counter Terrorism - Expecting the Unexpected

This guide is the result of a partnership between the business community, police, and business continuity experts of the United Kingdom. It advises on business continuity in the event and aftermath of an emergency and contains useful ideas on key business continuity management processes and a checklist. http://www.cabinetoffice.gov.uk/sites/default/files/resources/expecting-the-unexpected.pdf

Overseas Advisory Council (OSAC)

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 currently encompasses the 34-member core Council, an Executive Office, more than 110 Country Councils, and more than 6,800 constituent member organizations. www.osac.gov/

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. www.wood.army.mil/wood_cms/usacbrns.shtml

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. www.cbrne.army.mil/

U.S. Department of Health and Human Services' Office of Emergency Preparedness

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 dealing with 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 back to the United States from overseas armed conventional conflicts. www.hhs.gov/aspr/opeo/ndms/

U.S. Environmental Protection Agency Emergency Management

To ensure the Nation is better prepared for environmental emergencies, EPA is working with other Federal partners to prevent accidents as well as to 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. www.epa.gov/emergencies/index.htm

U.S. Food & Drug Administration – 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. www.fda.gov/Food/FoodDefense/Training/ALERT/default.htm

U.S. Food & Drug Administration – Employees FIRST

Employees FIRST is an FDA 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. www.fda.gov/Food/FoodDefense/Training/ucm135038.htm