FOR OFFICIAL USE ONLY

2010

Protective Measures Guide for the U.S. Lodging Industry

U.S. Department of Homeland Security

Homeland Security

American Hotel & Lodging Association
www.ahla.com

FOR OFFICIAL USE ONLY

Protective Measures Guide for the U.S. Lodging Industry

WARNING

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

Table of Contents

I. Introduction

Preventing terrorism, enhancing security, and ensuring resilience to 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 and key resources (CIKR). The U.S. Lodging Industry is designated as CIKR 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. As such, DHS developed the *Protective Measures Guide for the U.S. Lodging Industry* in collaboration with the American Hotel & Lodging Association to provide options for hotels to consider when implementing protective measures.

The guide provides an overview of threat, vulnerability, and protective measures designed to assist hotel owners and operators in planning and managing security at their facilities. It provides suggestions for successful planning, organizing, coordinating, communicating, operating, and training activities that contribute to a safe environment for guests and employees. In addition, when contemplating appropriate protective measures to implement, owners and operators should consider their own knowledge of the property's operations and vulnerabilities, as well as the general surroundings and its place within the community. When implementing appropriate protective measures, owners and operators should make use of additional resources, from local law enforcement and emergency management agencies to the security resources listed in the appendices of this guide.

This guide consists of contributions from the following partners:

- Accor Hospitality
- American Hotel & Lodging Association
- Bristol Hotel and Resorts
- Hilton Hotels Corporation
- HospitalityLawyer.com
- Hyatt Hotels Corporation
- InterContinental Hotels Group
- Interstate Hotels & Resorts
- Marriott International, Inc.
- The Peninsula New York
- Red Roof Inn
- Starwood Hotels and Resorts Worldwide, Inc.
- U.K. National Counter Terrorism Security Office
- U.S. Food and Drug Administration

Please note the following assumptions regarding the protective measures in this guide:

- This guide is not a complete source of information on protecting lodging facilities. Owners, operators, and security personnel should leverage the full range of resources they have available to them, and consider the specific nature of the threats, when responding to changes in threat condition levels.
- The protective measures delineated in this guide are presented for guidance purposes only; they are not a requirement under any regulation or legislation. In addition, because of the wide variety in the types, sizes, and locations of hotels, not all suggested protective measures will be relevant or applicable.
- The protective measures in this guide are based on practices that owners and operators across the country have employed at their facilities. The ability to implement them at any specific facility will vary.
- Hotel owners and operators should conduct a risk assessment at each individual property in order to decide which risks they consider applicable, and what protective measures they intend to employ.

2. Lodging Industry Profile

The U.S. lodging industry includes full-service hotels, limited-service hotels, resorts, conference centers, extended-stay hotels, vacation ownership, and convention hotels. Hotels range from stand-alone, multistory structures located in the downtown business district of a city to structures of only a few stories spread out over many acres in a resort setting. For the sake of brevity, this guide will refer to all lodging facilities as "hotels."

Many full-service hotels have restaurants, shops, and meeting rooms. Convention centers, shopping malls, sports facilities, and public transportation facilities may be adjacent to or integrated into the hotel facility. Hotels are also prominent in the growing number of multi-use districts that incorporate a wide range of facility types into a small, concentrated area.

Hotels generally have, and in some cases are required to have, both safety and security systems. Most hotels have systems in place for guest and employee safety, including fire protection sprinklers and smoke detectors. Safety systems available for hotels include automatic fire detection and alarm systems; automatic sprinklers; central annunciator panels; guest evacuation sound system; firefighters' voice communication system; smoke-proof, pressurized exit stairs; and emergency generator for alarm systems, lighting, and smoke exhaust. Security systems include closed-circuit television (CCTV), access control, and electronic key card readers.

2.1 Lodging Industry Overview

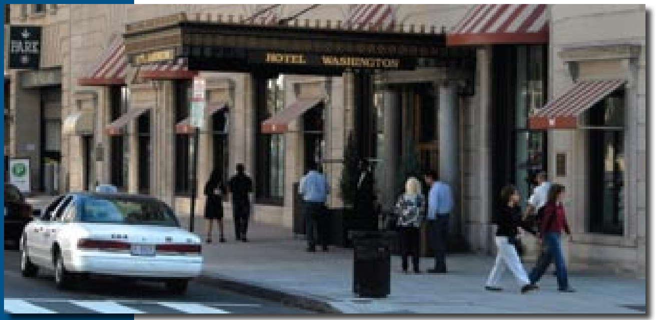
Hotels ordinarily exhibit certain characteristics that include the following:

- Continuous occupancy: Unlike many commercial facilities, hotels are occupied around the clock. People can eat, sleep, conduct business, and take part in entertainment activities within the same facility over multiple days.
- Emergency shelters: Hotels have been used as emergency shelters during times of natural disasters. Hotel companies have collaborated to find rooms for disaster victims and to make their hotels available in times of need.
- Self-contained: Some hotels maintain the capability to generate their own electrical power, and operate their own potable water filtration and waste-water treatment facilities.
- Just-in-time buyers: Many hotels do not maintain a large supply of resources. They often rely on online orders, and on the transportation and commercial distribution systems to deliver goods and services. Given this just-in-time delivery process, facilities are not required to store, prepare, or process fresh foods and supplies on site. However, this creates a problem for these hotels if they are to be used for shelter-in-place, as there may not be sufficient supplies available for the anticipated timeframe or number of people being sheltered.

2.2 Key Vulnerabilities of Hotels

Among the key vulnerabilities of the U.S. lodging industry are the following:

- Resistance to a fortress mentality: Many hotel companies must balance the need for enhanced security screening with positive customer perception. At the same time, increased security at hotels overseas is accepted and, in some locations, expected as a safety measure. There are many instances where U.S. hotels increase security and screening but this is usually done for an event or at the request of a special guest or client that is either staying at the hotel or participating in some function on hotel grounds.



- Unrestricted public access: Openness to the public is a feature common to hotels, and it contributes to their vulnerability. In general, hotels may have no security to screen guests for explosives or other weapons before they enter the facility.
- Differentiating between suspicious activity and tourist activity: Hotels are expected to have strangers flowing in and out of their properties daily. Tourists and terrorists are similar in that they both are inquisitive about the surroundings and they like to take photographs.
- Unrestricted access to service areas: In some hotels, because of fire exit requirements, some doors connecting service areas to public areas must remain unlocked at all times, allowing anyone access to the hotel's back of the house operations, which may include areas such as food storage, food preparation, utilities, chemical storage, etc.
- Unrestricted access to peripheral areas: Hotels can be vulnerable within their own parking lots or parking garages where guests and vehicles have access with little or no screening.

- ❍ Unrestricted access to areas adjacent to buildings: Most hotels have guest drop-off and pick-up points that are close to buildings. These points are generally not distant enough to prevent blasts from explosives packed in vehicles from inflicting significant damage to the buildings and guests. Generally, security personnel do not inspect vehicles stopped at these points for weapons or explosives.

- ❍ Access by suppliers, vendors, and maintenance workers to nonpublic areas: Many people other than hotel employees are given access to areas of the facility that are not open to the public. Such individuals include construction crews, maintenance personnel, and cleaning crews. In general, hotel security does not screen these individuals. These individuals and their vehicles often enter through loading docks, mailrooms, or service entrances that may not be secured or monitored.

- ❍ Staff turnover: There is a high turnover rate in housekeeping, wait staff, and security personnel at hotel and motels. This necessitates maintaining regular training for staff. Security is not the sole responsibility of the security staff; all hotel employees should emphasize and practice established security procedures and processes. Staff members that are not as familiar with their hotel's facilities and operations may be less likely to be aware of an unusual situation or individual.

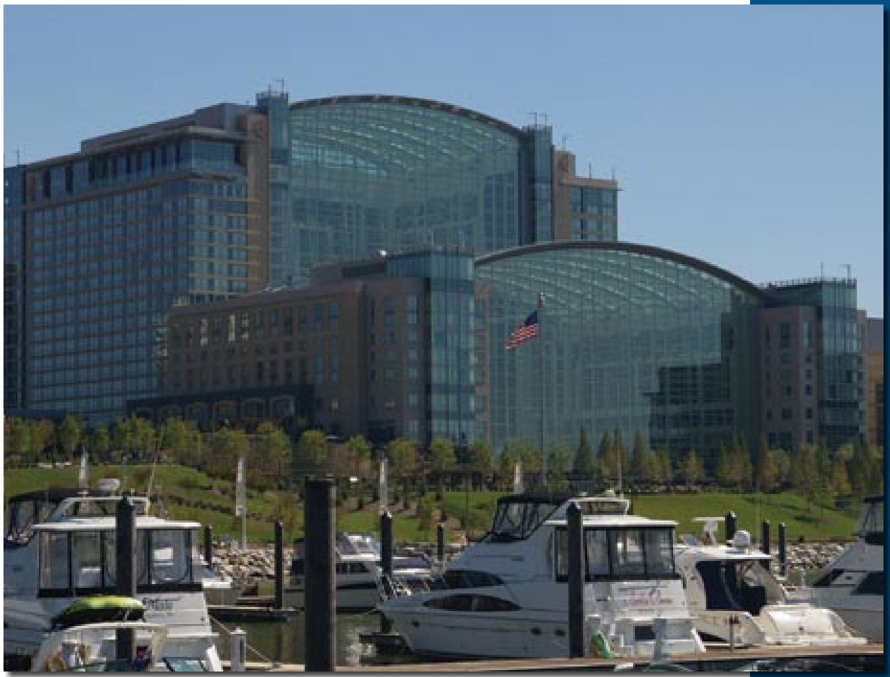
- ❍ Limited employee background checks: Many hotels, especially smaller ones, may conduct minimal or no background checks when hiring staff.

- ❍ Limited security staff: Many hotels have only a small security staff and rely mostly on local law enforcement to handle incidents. Larger hotels may have a larger security staff, sometimes under a contract arrangement with a private security firm. The extent to which these personnel are trained and equipped to deal with terrorist incidents varies widely.

- ❍ Lack of exercises for emergency plans: While some hotels, particularly the larger ones, have documented emergency operations plans, exercises of the plans are limited. It is difficult to interrupt normal business activities to conduct an emergency exercise. Coordination of hotel emergency efforts with those of local emergency responders may be lacking.

- ❍ Multiuse facilities: Hotels may be integrated with other facilities, such as malls, casinos, convention centers, universities, marinas, and airports. Each of these situations has its own site- and situation-specific vulnerabilities.

- ❍ Unprotected heating ventilating and air conditioning (HVAC) systems: In some hotels, access to the HVAC systems is not controlled or monitored; air intakes may be in publicly accessible areas. Additionally, HVAC equipment may not be



in secured rooms equipped with intrusion-detection equipment. In some cases, it may be necessary to shut down these systems to prevent outdoor-borne contaminants from entering the building as a terrorist may quickly contaminate a building with a biological or chemical agent by releasing it through the hotel's ventilation system.

- Unprotected utility services: Some hotels have not secured and do not monitor the utility services (e.g., electric power, natural gas, telecommunications, emergency generator and water supply) for intrusion.
- Structural configurations: Key configurations include atrium, tower, slab, and dispersed facility design. Building configurations with guest rooms clustered around a central core or around a multistory atrium may be more vulnerable to several types of threats than those facilities with individual units or low-rise clusters of rooms.
- Building height: Low-rise structures (one to two stories) are less vulnerable than high-rise structures. In structures with more than five stories, guest evacuation issues may be of greater concern in situations when elevators are unusable.

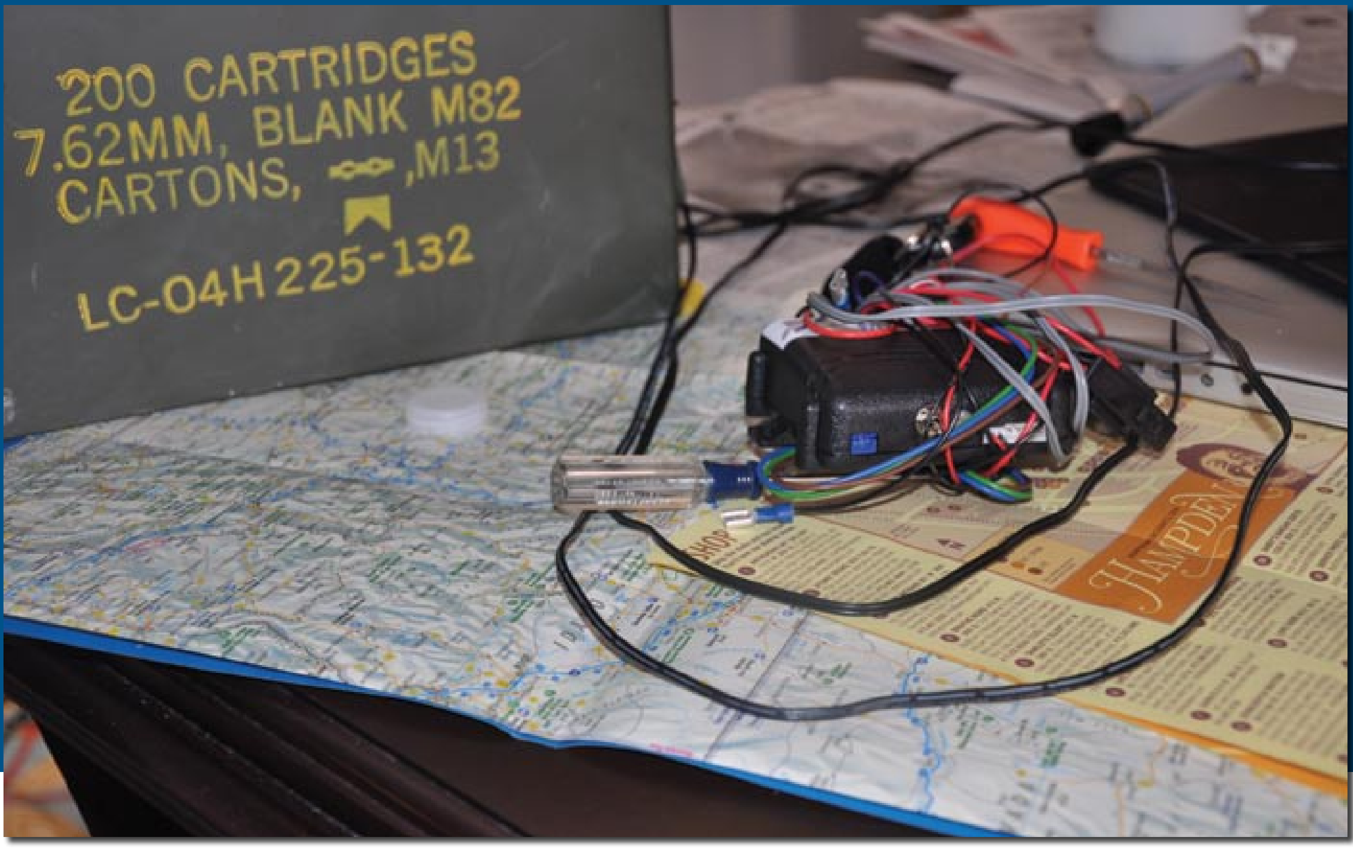
- Building designs are not security oriented: Many hotel buildings, particularly older ones, may not have been designed with security considerations in mind. Examples of such designs are those that include large areas of glass that is not shatter or blast resistant, structural supports that cannot handle large overpressures from explosives, and doors and windows that are not tamper-resistant.
- Multiple locations to place explosives or hazardous agents: Hotels have numerous locations where an explosives package (e.g., a backpack) or a container with hazardous agents can be left without being immediately noticed. These include trash containers, planters, counters, and decorative fixtures.

3. Terrorist Objectives

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 CIKR across the United States to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence in government leadership.

Inflicting 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. Disruption of the targeted site without inflicting actual damage can interfere with facility operations and tampering with facility products can render them dangerous or unusable. Theft of equipment, materials, or products can be intended to divert these resources to other uses or to reap financial gain from their resale. Theft of information can be intended to acquire insight that is not public information, gain data that can be used in carrying out attacks, or both. Because of terrorists' successful attacks on hotels overseas, terrorists' adaptability and their understanding of potential domestic consequences, and the vulnerabilities associated with hotels' open public access, it is important for hotel owners and operators to understand terrorist objectives and the types of threats that exist against the Nation's CIKR, so hotel owners and operators may take appropriate protective measures to reduce risk at their facilities.

4. Threat Streams and Hazards



Understanding threats and hazards, a hotel's potential vulnerability to them, and training security personnel and hotel staff to recognize and report potentially significant incidents, is the best way to manage risk.

For the purpose of this guide, manmade hazards are acts of terrorism, or any threat, activity, or attack with the element of human intent. Manmade hazards are distinct from hazards involving human error or negligence, which are included as "accidents" (Section 4.2).

4.1 Manmade Hazards

These attack methods are the manner and means, including the weapon and delivery method, an adversary may use to cause harm to a target. Terrorists utilize a variety of weapons and tactics 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. Manmade hazards include, but are not limited to:

4.1.1 Improvised Explosive Devices

IED used at hotel in Jakarta in 2009

An Improvised Explosive Device (IED), or homemade bomb, can be constructed from commonly available materials, construction explosives (e.g., dynamite), or stolen military-grade explosives. An IED also can be carried onto a facility by an individual serving as a suicide bomber or can be deposited in an unnoticed location for remote detonation. A suicide bomber is a person who intends to inflict destruction, injury, or death by concealing explosives on their person and detonating themselves to commit suicide. The near simultaneous bombings of two Jakarta hotels in July 2009 and the triple hotel bombings in Amman, Jordan, in 2005 are examples of IED usage.

4.1.2 Vehicle-borne Improvised Explosive Devices

Aftermath of VBIED at hotel in Islamabad, 2008

Vehicle-borne IEDs (VBIEDs) are loaded into a car or truck or onto a motorcycle. The vehicle can then be parked close to the facility and placed where large numbers of people gather, adjacent to the hotel perimeter, or driven through barriers and then detonated. VBIEDs are much larger and more dangerous than IEDs. Currently, VBIEDs are a common means of attack throughout the world. Surveillance often precedes IED and VBIED attacks. VBIEDs were deployed against the Pearl Continental Hotel in Pakistan in 2009 and the Marriott Islamabad in 2008.

4.1.3 Chemical Attack

Terrorists have exploited toxic chemicals as a weapon. Industrial chemicals can be transported by truck or by railroad to an area near a facility or large gathering of people and then dispersed by means of explosives. Chemical warfare agents (e.g., sarin or VX) are another weapon of concern. Although not readily available, historically they have been produced and used by terrorists. The most notable instance was the 1995 sarin attack on the Tokyo subway, which killed 12 people.

4.1.4 Biological Attack

Biological pathogens (e.g., anthrax, tularemia, plague) can cause disease and are attractive to terrorists because of the ability to cause mass casualties and the exhaustion of response resources. Biological agents can be dispersed into the atmosphere via crop-dusting aircraft or other airborne medium; can be introduced into a facility through its HVAC system; or can be 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 not appear for days or weeks afterwards. The most notable instance was letters distributed containing anthrax mailed throughout the United States in 2001, killing five people.

4.1.5 Nuclear or Radiological Attack

Weapons-grade nuclear material is very difficult to obtain. However, some sources of radiological materials are more readily available or easily delivered. Radiological materials include radioactive isotopes from a variety of sources, such as medical or industrial equipment. In radiological dispersion devices, often called "dirty bombs," terrorists can attach radiological materials to an explosive to create a wide area of contamination. Terrorists can also introduce radiological material or radiologically contaminated materials into a facility either directly or through the HVAC system.

4.1.6 Aircraft Attack

Both commercial and general aviation aircraft can be hijacked to deliver attackers, explosives, or hazardous materials to an area or facility. The aircraft itself (e.g., September 11th attacks) also can be used as weapons.

4.1.7 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. Prior to the 2008 terrorist attacks in Mumbai, terrorists used a fishing vessel and small boats to gain access to the city.

4.1.8 Cyber Attack

Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Information systems can be attacked with the intent of overloading the equipment (e.g., denial-of-service attacks). Information can be altered, stolen, or corrupted to render it unusable. Symantec Corp. reported that, in 2009, 75 percent of organizations suffered a cyber attack and lost an average of $2 million annually.

4.1.9 Sabotage (To include Insider Threat)

The disruption, damage, or destruction of a facility through sabotage and the introduction of hazardous materials into the facility are of concern. Sabotage may be perpetrated by employees or by outsiders. Employees may pose a greater threat as they have special knowledge of and access to facilities. A disgruntled employee may easily undermine even the best security plans. Al Qaeda operative Dhiren Barot tasked one of his terrorist cell members to work at a hotel to learn how to disable fire and security alarms.

4.1.10 Small Arms Assault (To include Active Shooter)

Small arms, including automatic rifles, grenade launchers, shoulder-fired missiles, and other such weaponry, can be used to target people (e.g., shooting of civilians) or facilities (e.g., standoff assault from outside a perimeter fence). An active shooter is an armed individual who uses deadly physical 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

Active Shooter, Mumbai 2008

their victims at random. Active shooter situations are unpredictable and evolve quickly. This tactic was employed during the attacks on the Pearl Continental Hotel in Pakistan in 2009, the Kabul Serena Hotel in 2008, and both the Taj Majal and Oberoi Hotels during the 2008 Mumbai terrorist attacks.

If there is an active shooter in your vicinity, quickly determine the most reasonable way to protect your own life. Visitors, guests, and other employees are likely to follow the lead of employees and managers during an active shooter situation.

Active Shooter, Mumbai 2008

1. **Evacuate.** Have an escape plan and route in mind, leave your belongings behind, and keep your hands visible.
2. **Hide out.** Hide in an area out of the active shooter's view, block entry to your hiding place, and lock the doors.
3. **Take action.** As a last resort and only when your life is in imminent danger, attempt to incapacitate the active shooter. Act with physical aggression and throw items at the active shooter.

For additional information, please visit the DHS Commercial Facilities Sector Training and Resources Web site, www.dhs.gov/cfsector, for the *Active Shooter-How to Respond* materials. The materials include 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. See Appendix E: Additional Federal Resources – Web sites for details.

4.1.11 Arson

The intentional and malicious setting of fires can be accomplished by using highly flammable materials (e.g., gasoline) in a facility. The flammable materials often referred to as accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson also could be used in conjunction with other forms of attack such as a small arms assault, or can be a second order effect of another form of attack such as an IED.

4.1.12 Surveillance

Indicators of surveillance include persons or unusual activities near the hotel intended to gather information about the facility or its operations and protective measures. Suspicious activity could be an indicator of a potential terrorist attack and should be reported to the police. The following activities may be relevant to hotels:

- Significant interest being taken inside a hotel near Closed Circuit T.V. (CCTV) cameras; elevators and emergency exits; and outside of a hotel, including parking areas, entrances, and parking garages.

- Persons carrying observation equipment, including global positioning systems (GPS) in or near a hotel over an extended period of time. GPS may assist in the positioning of weapons.
- Persons questioning hotel employees about off-site practices, facility supporting infrastructure, or about the number and routines of staff, guests, or VIPs in the hotel.
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
- Items (e.g., packages, luggage) and vehicles left unattended.
- Series of false alarms, potentially indicating testing of security systems and surveillance of procedures and response.
- Attempts by individuals to gain access to restricted areas.
- Unusual telephone calls or e-mails questioning specific security measures present at the facility, sometimes under the guise of someone considering staying at or hosting an event at the facility.
- Any other activity that is inconsistent with the nature of the building.

4.2 Accidents

Hotels must 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 hotel perimeters also could affect facilities.

4.3 Natural Disasters

A natural disaster such as a hurricane, tornado, earthquake, or severe storm may occur with or without warning and severely impact operations at your hotel. Though the majority of this document will focus on manmade-related incidents, hotels also should plan for all hazards, including natural disasters.

5. Protective Measures

Protective measures include 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:

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 greatest risk at any facility may be complacency. The implementation of protective measures at any time involves the commitment of resources in the form of people, equipment, materials, time, and money. Facility owners 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 this decision process, a risk-based protective posture is recommended. DHS recognizes the three following 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.
- **Vulnerability:** Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat.
- **Consequence:** Effect of an event, incident, or occurrence.

For the purpose of this guide, the protective measures offered are general measures, or measures to follow if there is a credible threat to your facility, geographic area, or industry. When available intelligence allows, DHS alerts are supplemented by information on the threat stream(s) most likely to be used by terrorists. This information may or may not be very specific, may or may not identify geographic areas of concern, and may or may not offer a time when attacks might be expected. This level of uncertainty is inherent in dealing with terrorist threats and must be factored into decisions on committing resources to the implementation of protective measures.

However, each hotel should conduct their own risk assessment and tailor their plans according to the risk at their own facility. Risk assessments are discussed in greater detail in Section 5.1. Hotels are also encouraged to have a scalable approach to managing risk, with 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.

The protective measures described below are designed to provide information and assistance to hotel owners, site managers, local law enforcement, and State and local homeland security agencies in making decisions on managing risk. These suggested measures are collated from infrastructure-specific guidance and from experience in a number of localities from across the country.

The protective measures described below are grouped into the following categories:

- Planning and Preparedness
- Incident Response
- Personnel
- Access Control
- Barriers
- Communication and Notification

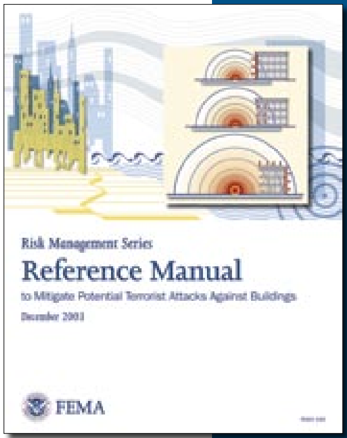
- ❍ Monitoring, Surveillance, Inspection
- ❍ Information Security/Cybersecurity
- ❍ Infrastructure Interdependencies

Additional protective measures are included for consideration for use during periods of high alert, when a higher state of readiness may be required at a property, locality, region, or all hotels nationally.

The ability to implement protective measures at any specific facility will vary. For smaller or independent properties without large staffs or corporate resources, not all suggested protective measures will be relevant or applicable.

Additional resources for hotels include the Federal Emergency Management Agency (FEMA) Security Risk Management Series publications, a series directed at providing design guidance for mitigating multihazard events. (See Appendix E: Additional Resources – Web sites for more detail).

5.1 Planning and Preparedness



Risk Management Series

Reference Manual

to Mitigate Potential Terrorist Attacks Against Buildings

December 2003

FEMA

Hotels should conduct threat, vulnerability, and risk assessments to determine a property's relative levels of risk, and to help identify the best and most cost-effective mitigation measures for their own, unique security needs. (*FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* discusses the assessment process, asset value assessment, threat/hazard assessment, vulnerability assessment, risk assessment, and risk management. The publication also provides a Building Vulnerability Assessment Checklist and can be found at http://www.fema.gov/plan/prevent/rms/rmsp426. FEMA 426 is a particularly helpful reference manual for new buildings during the design process, as well as for existing buildings going through a renovation).

Security audits should be conducted on a periodic basis. Include assessments of other critical activities and operations in the vicinity (for example, airports, chemical plants, government buildings, pipelines, and rail lines) to determine if there is any potential for them to cause increased security risks to the hotel. Based on these analyses, develop a comprehensive security plan, emergency response plan, and business continuity plan for the hotel. (See Appendix E: Additional Resources – Web sites – practical steps and easy-to-use templates, as well as useful links to resources providing more detailed business continuity and disaster preparedness information, can be found at http://www.ready.gov/business/index.html.)

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

Security and Personnel Responsibilities

❍ Designate a supervisory-level person to develop, implement, and coordinate all security-related activities. Previous security, law enforcement, and facility management experience is recommended.

❍ Consider forming an interdisciplinary stakeholder group, comprised of the hotel's various departmental managers, to consult with the person in charge of the security planning process.

❍ In addition to the designated security leader, who will likely work with authorities in the event of an incident, consider appointing other reliable team members with additional roles.

Useful roles and whom to assign the roles to may include:

- Final decision making authority and managing all response efforts – General Manager
- Coordinate communication with guests, patrons, and visitors – General Manager or Front Desk Supervisor

- Damage assessments – Engineering
- Grant access and escort first responders or utilities personnel to mechanical or restricted areas – Engineering
- Assess financial needs during the recovery and evaluate loss – Controller (Finance)
- Provide staff support, keep staff informed, manage schedules, and contact families in the event of emergencies – Human Resources
- Communicate with external audiences – Public Relations/Marketing
- Control both vehicle and pedestrian traffic flow, safeguard luggage, and restrict access in and out of the hotel for emergency authorities – Security, Doorman, Front Desk Agent
- Safeguard credit cards and financial records – Accounting, IT

❍ Involve employees at several levels in security planning. Consider third-party evaluation and verification of the plans.

❍ Maintain regular communication with local law enforcement and first responders, Federal and State law enforcement and anti-terrorism agencies, public health organizations, and hotel industry organizations to enhance information exchange, clarify emergency responses, track threat conditions, and support investigations. The hotel's security and mutual aid agreements, critical information about the hotel (including, floor plans, location of emergency equipment, and notification and contact lists) should be shared with local law enforcement and emergency responders. Host emergency responder meetings on site whenever possible.

❍ Develop policies and procedures for dealing with the media and the general public in the event of an incident to apprise them of the situation and to prevent rumors and panic. Identify the people who will have responsibility for media interactions, and devise templates for messaging prior to incidents.

Emergency Preparedness

❍ Consider creating checklists, pre-recorded announcements, and standard operating procedures for incidents, including but not limited to:

- Severe weather (flood/hurricane/tornadoes/winter storm)
- Bomb threats
- Civil disorder or disturbance
- Fire or explosion
- Hazardous material (HAZMAT) or chemical spill
- Hostage taking
- Active shooter
- Structural collapse

- Suspicious item or packages
- Pandemic flu, viral contamination, or quarantine
- Power failure
- Multiple, simultaneous events (i.e. severe weather and power failure)

○ Ensure that adequate equipment and supplies are available to support emergency response requirements.

- Check the status of all emergency response equipment and supplies on a regular basis. Store emergency supply kits in areas where they are readily accessible to employees or emergency responders. Provide adequate security for emergency response equipment, facilities, and personnel. Do not leave emergency vehicles or equipment unattended or unsecured.
- Regularly inspect and replace items such as batteries, flashlights/glow sticks, blankets, bolt cutters, bull horns, duct tape, emergency vests, fire extinguishers, first aid kits, rope, battery-operated radios, masks, and master keys.
- Consider preparing hard hats and emergency vests labeled with the hotel's name and title of each of the crisis management team member. This will allow for easy identification by guests and first responders in an emergency that encompasses other facilities.
- Determine the need for personal protective equipment (PPE) for employees (e.g., toxic material detectors, breathing apparatus). Deploy equipment for ready use in the event of an incident.

○ Consider the installation of an emergency operations center or emergency command center that can be used to coordinate resources during an incident. If necessary, consider a backup center or a mobile capability for use in the event the primary center is disabled.

○ Hotel security leaders should meet with first responders prior to an emergency. Involve first responders in exercises to ensure that they have up-to-date floor plans and information about hotel logistics and emergency procedures in the event they need to respond to an emergency.

○ Develop procedures for shutting down the hotel in the event the threat is deemed too serious to continue operations.

○ Develop a notification protocol that outlines who should be contacted in emergencies. Designate who is to contact whom within the hotel and with outside organizations. Provide a contact list to all who might need it and keep the list up-to-date. Regularly test notification protocols through drills and exercises.

○ Develop a notification protocol for guests that communicates the current situation during an emergency and what they should do (i.e., evacuate or shelter-in-place).

○ For larger hotels, consider forming an Emergency Response Team or Teams. Designate specific responsibilities for each team and define when each would activate or deploy (regular business hours, evening/overnight, holidays) to avoid confusion during an incident. Selection of team members would ideally focus on those who could most easily deploy based on schedule and transportation capabilities of the individual.

- ■ Ensure that an adequate number of emergency response personnel are on duty and on call at all times.
- ■ Ensure that there are backup personnel who can execute emergency response functions in the event that primary personnel are unavailable or incapacitated.

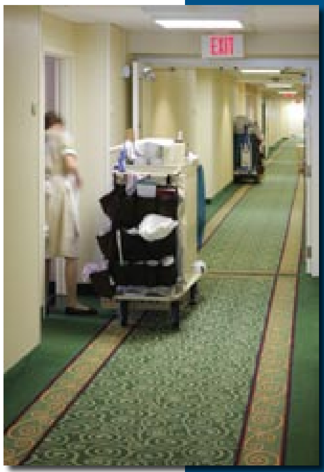
Security Procedures

- ❍ Develop Operations Security (OPSEC) procedures to cover routine security activities by all employees.
- ❍ Review, test, and update all plans annually, including the security plan, emergency response plan, and business continuity plan.
- ❍ Keep copies of the security and emergency response plans in redundant locations. Ensure that the plans are protected from unauthorized disclosure but readily accessible by authorized staff.
- ❍ Relocate sensitive or critical items (e.g., specialized equipment, important records) to areas of the hotel with greater physical security.
- ❍ Conduct regular exercises with hotel employees to test the security and emergency response plans, and to ensure that adequate resources are available to implement the plans and that all hotel operation units can implement their responsibilities under the plans.
- ❍ Develop policies and procedures for dealing with hoaxes and false alarms so as not to burden hotel operations.
- ❍ Establish the capability to collect and interpret available threat intelligence from Federal, State, and local agencies. Maintain constant awareness of current threat condition and available intelligence information. As part of the security plan, establish procedures to implement additional protective measures as the threat level increases. Also, establish procedures for returning to lower security levels as the threat decreases. Alert local law enforcement and emergency responders of measures being implemented.
- ❍ For hotels without a dedicated security staff, or those who desire additional resources, request that local law enforcement add the hotel to their patrols. Additionally, many agencies (e.g. DHS, State homeland security, local law enforcement agencies) will conduct site security assessments at the request of hotel owners.

Accountability

- ❍ Have a system in place to maintain accountability for associates, registered guests, guests with special needs, tenants, and contractors.
- ❍ Ensure that one or more hotel employees, including a senior security official who is familiar with the emergency plan, are available for deployment at all times.

Good Housekeeping



Not only will housekeeping practices improve the ambiance of a hotel, they may reduce the possibility that suspicious items may be left behind and unnoticed. Housekeeping may reduce the risk at a hotel through the following:

- ❍ Ensure prompt cleaning of waste facilities.
- ❍ Consider the use of clear waste disposal bags so staff may examine waste for suspicious items.
- ❍ Ensure that landscaping and external aesthetics, trash cans, and mailboxes do not provide hiding places.
- ❍ Keep public, communal, and external areas as clean and well lit as possible, particularly exits, entrances, reception areas, stairs, and hallways.
- ❍ Place trash receptacles as far away from the hotel as possible. Secure dumpsters and other trash receptacles to prevent the hiding of explosives or other hazardous materials and to prevent unauthorized access to discarded papers and records.
- ❍ As many hotels have on-site maintenance facilities, appropriate storage should be considered for the following materials:
  - Fertilizers for lawns and grounds.
  - Oxidizers for pools.
  - High-pressure flammables in the maintenance shops.
  - Fuel storage for emergency power sources.
  - Propane storage tanks.

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

- ❍ Review and implement actions specified in the security and emergency response plans; adjust the plans as necessary to deal with specific threat information.
- ❍ Activate hotel emergency operations center as appropriate.
- ❍ Review available threat information and determine whether the hotel should be closed. If the determination is to close the hotel, evaluate criteria for when the hotel should be reopened or restored to full operation.

5.2 Incident Response

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

General Measures

- ❍ Consider the use of an incident activity log, which allows for the capture of events as they occur. Designate an employee to ensure accuracy of the log.

- Understand the procedures or necessary responsibilities for off-site personnel to gain access to the hotel or affected area in the event of an incident that may restrict access to the hotel or the surrounding area.
- Develop a list of key personnel who are pre-approved to enter the hotel after an incident and assist with recovery activities.
- Maintain an emergency shutdown list if needed to isolate the hotel from potential contaminants; emergency shutdown capability should be available at all times.

- Review unified incident command procedures for responding to an event with local law enforcement, emergency responders, and government agencies.
- Establish an emergency operations center or emergency command center that can be used to coordinate resources during an incident. Ensure that the command center has adequate resources to conduct emergency operations, including but not limited to, communications equipment, televisions, office supplies, and computers.
- Provide training and equipment to emergency response personnel to enable them to deal with terrorist-related incidents (e.g., chemical; biological and radiological agents; suicide bombers). Conduct regular drills and tabletop exercises with emergency response teams. Involve local emergency responders in drills and exercises.
- Ensure that copies of essential items such as floor plans are kept off site.
- Encourage employees to participate in community and other outside organization emergency preparedness and response training.
- Develop plans to provide counseling to employees in the aftermath of an incident.
- Implement procedures for capturing lessons learned and developing revised response plans after an incident.
- Identify entry and exit points to be used in emergencies. Ensure that they are free of obstructions and can be fully utilized. Inspect these points regularly for signs of tampering and intentional obstruction. Train all employees on the location of these points.
- Many of the casualties in terrorist attacks are caused by flying glass, especially in modern buildings. Consider protective options that will mitigate the effects of flying glass, such as anti-shatter film, glazing protection, or laminated glass.
- 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 hotel buildings and areas where large numbers of people congregate.

Searches, Evacuations, and Sheltering-in-Place

❍ Establish procedures to identify security responsibilities and a chain of command for responding to an incident. Consider establishing a response team in the event of evacuation, shelter-in-place, and search situations.

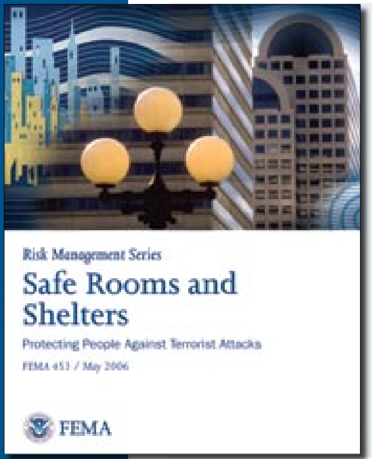
❍ Establish procedures for dealing with people who have special needs (e.g., physical disabilities, non-English speaking, and Limited English Proficiency (LEP) individuals).

❍ Include evacuation as part of the security plan. Events that could necessitate an evacuation in the hotel or at a nearby facility include suspicious packages, suspicious vehicles, or another incident identified by local authorities. Evacuation plans should:

- Consider the need to evacuate in all types of weather and during all times of the day.
- Include areas such as each hotel floor, stairways, exits, elevators, meeting/banquet rooms, any public or leased areas, back of house areas, offices, kitchens, and indoor and outdoor amenities.
- Ensure that the hotel has smoke-proof, pressurized exit stairways.
- Consider scenarios for full evacuation, partial evacuation, and internal or shelter-in-place, taking into account "adequate time for full evacuation" versus "adequate space for shelter-in-place," instructions from local authorities, and the potential danger of outside conditions.
- Identify assembly points where employees and others at the hotel can gather for a coordinated evacuation and for "head counts" to ensure all have been evacuated. Make staff aware of assembly point locations. Identify alternate rallying assembly points in the event primary assembly points are inaccessible during an incident. Consider mutual agreements with nearby facilities to use each other's locations when necessary.
- Identify alternate transportation routes for employees and others at the hotel to use during evacuations. Test the routes by means of drills and exercises.
- Ensure people are moved away from other potentially vulnerable areas when planning evacuation routes in response to attacks; consider that a secondary device may be planted.

❍ Establish procedures for shelter-in-place situations.

- Designate shelter-in-place locations where people can congregate in the event of an outdoor release of hazardous materials. The goal is to create areas where outdoor air infiltration is very low. Usually such rooms will be in the inner part of a building in an area with no exterior windows. *FEMA 453: Safe Rooms and Shelters: Protecting People from Terrorist Attacks* provides guidance for engineers, architects, building officials, and property owners to design shelters and safe rooms in buildings and can be found at http://www.fema.gov/library/viewRecord.do?id=1910 (See Appendix E: Additional Resources – Web sites).



Risk Management Series

Safe Rooms and Shelters

Protecting People Against Terrorist Attacks

FEMA 453 / May 2006

FEMA

- Include procedures for protecting guests from outside contaminants including turning off HVAC units, closing or sealing windows, and shutting down elevators to minimize the air draft effect inside elevator shafts.
- Ensure the hotel is stocked adequately with food, water, and supplies to accommodate the number of people who might need to use them.
- Monitor communication with law enforcement to determine when the emergency has ceased.

❍ Prepare search plans and train staff to ensure that all grounds are searched thoroughly, bearing in mind that law enforcement or first responders cannot search a hotel as quickly or as thoroughly as a member of its own staff or security team. Consider dividing the facilities into manageable sections. Also develop plans to search all grounds in response to an incident and after an evacuation. Staff familiar with the hotel will need to search the grounds in order to ensure safe re-entry into the hotel.

- Search teams should be divided into teams of at least two for safety purposes, and should be assigned areas that are accessible in light of the team members' physical abilities.
- Secure rooms once they have been searched. Consider using an easily visible marking system such as reflective tape or glow-in-the-dark stickers to identify rooms that have already been searched. Rooms that have been searched should be secured immediately to avoid unauthorized access and protect guest belongings.
- If rooms with young children are identified, a more thorough search (i.e. behind curtains, in closets) may be required as children often hide when scared.

❍ Establish an accountability plan to ensure all guests and employees evacuate safely. Account for guests with special needs.

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

❍ Review and implement actions specified in the security and emergency response plans including expanding search, evacuation, and shelter-in-place capabilities. Adjust the plans as necessary to deal with specific incident conditions.

❍ Activate hotel emergency operations center as appropriate.

❍ Cancel or delay leave or travel for critical hotel personnel.

❍ Pre-position emergency response personnel and equipment to locations that would enable rapid response to an incident.

❍ Review procedures with employees assigned to shut off utilities (e.g., electricity, water, natural gas, etc.) in the event of an incident.

- Review procedures with employees assigned to back up all accounting transactions, employee attendant records, guest lists, and registration cards.
- Review cash flow and amount of capital available to be used during emergency and post- emergency.

5.3 Personnel

A trained and attentive staff is an essential element to protective measures. Knowing that they have the confidence of their employers is an essential aspect to encouraging employees to report suspicious activity. Every staff member should be encouraged to report out-of-place items. Reports should be treated seriously, with respect, and as a contribution to maintaining a safe workplace and business.

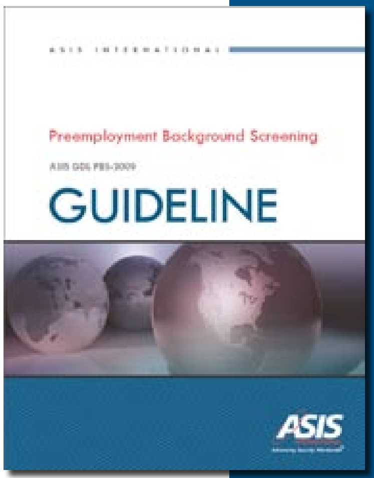
A trained workforce is essential to ensuring that appropriate actions are carried out in the event of an emergency. Staff also should be trained to remain calm as guests will look to them for guidance in an emergency.

Just as training staff is important to protecting a hotel, ensuring that competent and credible staff are hired in the first place is also important. As laws vary from state to state, consider conducting the maximum measures allowed by state law, particularly in hiring for sensitive positions.

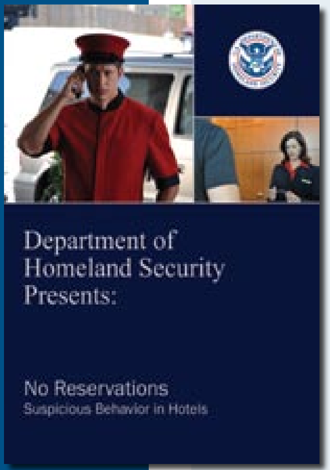
Employees

The following measures may be considered in regards to employment and staffing issues:

- Conduct background checks on all employees. Consider verifying identity, employment history, criminal convictions, financial history, and history of overseas criminal activity. (The ASIS Preemployment Background Screening Guideline (2009) is a resource that aids U.S. employers in understanding and implementing the fundamental concepts, methodologies, and related legal issues associated with pre-employment background screening of job applicants, and is available for purchase at, http://www.asisonline.org/guidelines/published.htm).
- Conduct more detailed checks on those who will have access to critical assets.
- Develop a list of disqualifying factors that can be used to reject an individual.



- Ensure that contract companies used by the hotel have the same rigorous standards for pre-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 recognizing situations that may pose a security threat (e.g., suspicious behavior, persons without proper employee identification, persons carrying unusual packages, unattended/suspicious vehicles



and packages, and strange odors or liquids). *No Reservations: Suspicious Behavior in Hotels* is a DHS-produced video designed to raise awareness for hotel employees by highlighting the indicators of suspicious activity. The video can be found at DHS's Commercial Facilities Sector Training and Resources Web site, www.dhs.gov/cfsector. See Appendix E: Additional Resources – Web sites for details.

- Security awareness and response plan Standard Operating Procedures (SOPs) that are to be used for different types of incidents.
- Contact and notification protocols for suspicious items, suspicious situations, and emergencies. Contact information for all key staff should be easily accessible.
- Practice caution in providing hotel information to outsiders.
- Procedures to provide for the safety of employees during a security incident including searches, emergencies, and evacuations.
- Searches of vehicles, persons, baggage, and packages.
- Appropriate actions to conduct upon receiving bomb threats.

- ❍ Maintain up-to-date security training with regular refresher courses. Maintain records of employee training that have been completed.
- ❍ Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., working irregular hours, attempting to access restricted areas, or carrying unusual packages). Maintain awareness of any unusual patterns of employee illness that might indicate exposure to a toxic agent.
- ❍ Review the personnel files of recently terminated employees to determine whether they pose a security risk. Take appropriate actions to mitigate the risk.

Security Staff

- ❍ Maintain an adequately sized, equipped, and trained security staff. Ensure that an appropriate number of security personnel are on duty or on call in the event of an incident. Determine the availability of security staff reinforcements that would be deployed during heightened threat conditions. Conduct more rigorous background checks on security personnel.
- ❍ Develop a procedure and location for detaining and questioning persons exhibiting suspicious behavior and violating security regulations. Train security staff in appropriate methods for handling these people.
- ❍ Conduct regular drills and exercises with the security staff. Involve local law enforcement and other agencies as appropriate.
- ❍ Alter the appearance of security personnel (e.g., changing uniforms, vests, plain clothes) to disrupt terrorist planning.
- ❍ Develop a security staff schedule that includes random patrols of the grounds and facilities.

Contractors, Vendors, Concessionaires, Temporary Employees

- ❍ Provide security information and training to contractors, vendors, concessionaires, and temporary employees either operating out of, visiting, or temporarily working at the hotel. Advise them to be alert to suspicious activity or items, and instruct them on how to report such incidents.
- ❍ Require contractors, vendors, concessionaires, and temporary employment agencies to vouch for the background and security of their personnel who will be at the hotel.

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

- ❍ Provide additional training and reminders to employees about the security situation. Provide refreshers on SOPs to be used for different types of incidents.
- ❍ Increase security staff presence by using overtime and additional personnel. Increase frequency of patrols. Increase patrols and inspection of unstaffed and remote parts of the hotel. If necessary, request additional security staff support from local law enforcement.
- ❍ Extend patrols to a wider perimeter around the hotel property in coordination with local law enforcement.
- ❍ Activate a security command post (within the emergency operations center).
- ❍ Have employees vary their routines to avoid predictability.

5.4 Access Control

Access Control protective measures can pertain to the physical access to a hotel by guests, patrons, visitors, employees, contractors, vendors, temporary employees, third parties, vehicles, and mail. It includes the following:

General Measures

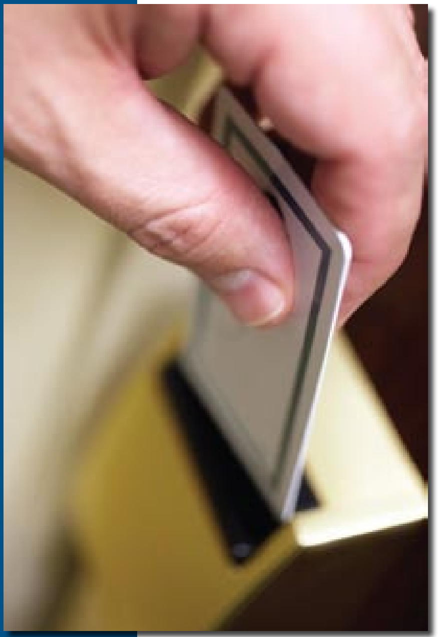
- ❍ Define the hotel perimeter and identify sensitive or critical areas including processing areas, control rooms, communications centers, computer server areas, shipping areas, mail rooms, fuel or chemical storage tanks, pipelines and valves, and utility service areas within the hotel that require special access control for pedestrians and vehicles. Maintain the minimum number of hotel access points needed to meet operational and safety requirements. Where necessary, design layered access points that provide multiple opportunities to permit or deny entry. Where possible, locate sensitive equipment and assets in the interior of the hotel. Evaluate and select access control measures for each access point.

❍ Provide appropriate signage to identify access points for hotel guests, vehicles, and pedestrians. Signs may clarify restricted access; however, refrain from identifying sensitive areas with signage including those with critical utilities. Consider signs in multiple languages where necessary.

❍ Provide security guards at key access points. Train guards to identify pedestrians and vehicles that are permitted access. Train guards, and all staff, on procedures for denying access. Provide additional security to hotel buildings and other assets that are on the hotel perimeter where they may be more open to unauthorized entry attempts.

❍ Strictly enforce all access control measures including locking of rooms not in use and enforcing an employee badge check on a continuing basis. Allow no exceptions.

❍ Check guest identification upon check-in and when requesting additional room keys or information.



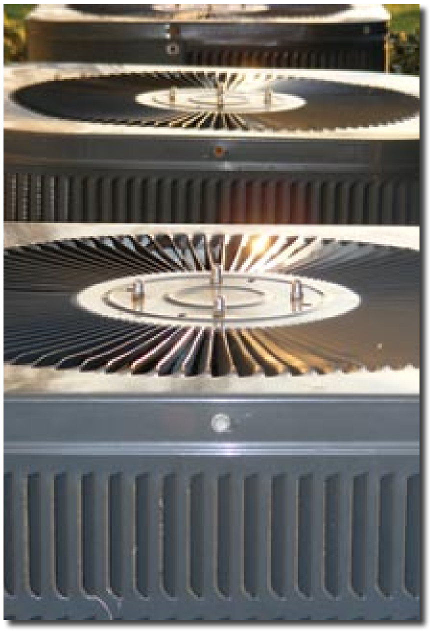
❍ Implement rigorous key control procedures. Track holders of all keys. Secure master keys and make sure they do not leave the premises. For facilities with non-electronic keys, maintain a strict control program. If guest keys are lost or not returned at checkout, or other security issues occur, make sure to change locks or tumblers immediately. Maintain logs of associate keys and that only the minimum number of keys necessary are distributed.

❍ Secure accessible windows with quality key-operated locks. The locks should be checked regularly.

❍ Regularly inspect and test all access control devices (e.g. electronic key readers).

❍ Prevent public access to building roofs, HVAC intakes, and mechanical rooms. Provide access control measures for ladders, awnings, and parapets that give access to building roofs, HVAC systems, and other critical equipment. Ensure that nearby foliage cannot be used to gain access to the roofs of buildings.

❍ Prevent contamination to the entire hotel by deterring and blocking access to the ventilation system. Install controls for barriers to HVAC systems (e.g., intake screens, filters) to prevent the introduction of chemical, biological, or radiological agents into the hotel. Where needed, provide positive pressure in the building to prevent contaminants from entering. Train staff in emergency shut-off procedures for HVAC systems.



❍ Provide adequate door and window locks, barred entryways, fencing and gate locks, timed closure devices, and other access controls to buildings, rooms, elevators, shipping and receiving areas, storage tanks and bins, emergency generator utility access points (e.g., manholes and HVAC systems), hazardous materials (e.g., fuels and pool chemicals) storage areas, and other areas where access is to be limited. Add intrusion-detection systems and alarms as appropriate. Utilize greater security controls (e.g., card swipe locks, biometric identification) in sensitive or critical areas. Maintain a log of those accessing these areas.

- ❍ Screen, seal, or secure all utility penetrations of the hotel's perimeter to prevent their use as access points for unauthorized entry into the hotel (e.g., utility tunnels, corridors, manholes, and storm water runoff culverts, etc.).
- ❍ Secure all tools that could be used to force entry into a secured area, building, or room (e.g., bolt cutters, hacksaws, and cutting torches).
- ❍ Restrict the storage of luggage to locations away from areas where large numbers of people congregate.

Employees

- ❍ Issue photo identification badges to all employees. Require that the badges be displayed and verified to gain access to the hotel. Occasionally test the response of employees to unauthorized persons at the hotel. During times of heightened alerts, require that employee badges be worn at all times in the hotel. 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 hotel and sensitive areas.
- ❍ Develop a policy for lost employee identification badges.
- ❍ Collect employee identification and keys when employment is terminated and consider changing locks. If exit interviews are conducted with a terminated employee, ensure these steps are part of the exit interview checklist, as well as updating staff contact lists to reflect changes.
- ❍ Implement a policy that addresses off-duty personnel accessing sensitive areas.

Contractors, Vendors, Temporary Employees, and Third Parties

- ❍ Issue special identification badges to contractors, cleaning crews, vendors, temporary employees, and third parties. Require that the badges be displayed and verified to gain access to the hotel. Require that badges be worn at all times in the hotel. Collect all badges when their visit is complete.
- ❍ Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confined by prior arrangement. Require contractors, vendors, and temporary employees to sign in and sign out.
- ❍ Require that terminated contractors, vendors, and temporary employees return employee identification badges and keys.
- ❍ Encourage employees to develop a familiarity with contractors, vendors, and temporary employees. Have them question any unusual or unrecognized people and report incidents to hotel security personnel.
- ❍ Escort all non-employees when they are in sensitive or critical areas. Escort maintenance workers throughout their service visit and visually inspect their work before final acceptance of service.
- ❍ Consider a policy regarding requests for security surveys by foreign insurance companies.

Vehicles and Parking

❍ Locate general parking in areas that present the fewest security risks to personnel. Direct adjacent public parking to more distant or better-protected areas, segregated from employee parking and away from the hotel, where applicable. Consider using centralized parking and a shuttle service to keep vehicles away from critical assets.

❍ Review vehicle traffic patterns inside the hotel grounds. To the extent possible, limit vehicular entry/exit to a minimum number of locations.

❍ Keep vehicles away from sensitive or critical assets and from areas where large numbers of people congregate. 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.

❍ If possible, prohibit parking beneath or within a building. If parking beneath a building is unavoidable, limit access to the parking areas and ensure they are secure, well-lit, and free of places of concealment.

❍ Do not permit uninspected vehicles to park under a building or within an exclusion zone. If parking within the building is required, apply the following restrictions:

- Public parking with ID check;
- Company vehicles and employees of the hotel only;
- Selected company employees only, or those requiring security.

❍ If parking is open access, conduct more rigorous searches of vehicles. Questioning can include asking drivers to confirm guest rooms, length of stay, purpose of visit, and proof of vehicle ownership.

❍ Maintain a database of employee-owned vehicles; issue parking permits for designated areas.

❍ Lock all hotel vehicles and park them in a secure area when not in use.

Mail, Shipment, Deliveries

❍ Screen all deliveries to the building, including U.S. mail, commercial package delivery services, and packages for guests who do not check in.

❍ Train mailroom and receiving personnel to recognize suspicious mail, packages, shipments, or deliveries, and instruct them in the procedures to follow. (See Appendix B: Suspicious Mail or Packages and Appendix E: Additional Federal Resources – Web sites)

❍ Accept deliveries and shipments only from known shippers, vendors, or guests.

❍ Designate an area for processing mail that is separate from central ventilation.

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

- ❍ Tow vehicles parked illegally or in unauthorized spaces.
- ❍ Consider the use of intrusion detection systems with central monitoring capabilities.
- ❍ 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 all essential contractors, vendors, and temporary employees while at the hotel.
- ❍ Restrict parking to areas away from critical assets. Evaluate the closure of underground or under-building parking lots.
- ❍ Redirect mail, shipments, and deliveries to areas distant from sensitive or critical assets. Accept deliveries only during daytime hours.
- ❍ Require that employee badges be worn at all times in the hotel.
- ❍ Review available threat information and determine whether the hotel should be closed. If the determination is to close the hotel, evaluate criteria for when the hotel should be reopened or restored to full operation.

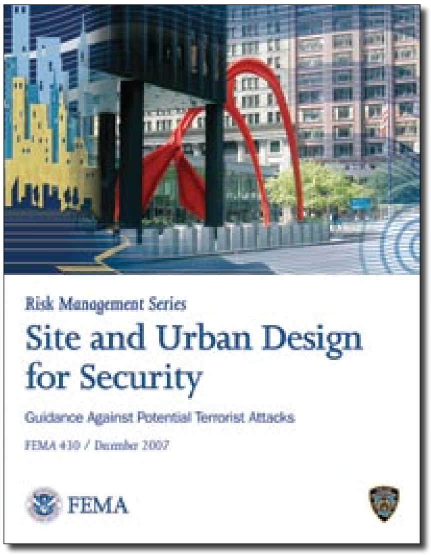
- ❍ If the decision is made to keep the hotel open, institute the following practices:
  - Reduce access to an absolute minimum.
  - Do not allow access to the back of the house to non-employees.
  - Halt all contractor work.
  - Accept no non-essential mail, shipments, or deliveries.

5.5 Barriers

A physical barrier is a means of establishing a controlled access area around a building or asset. The use of physical barriers and controls can serve a variety of purposes at a hotel and do not necessarily have to detract from its physical appearance. Barriers can designate a space or provide legal boundaries for a property, control the entry and traffic flow of both pedestrians and vehicles, provide standoff distance from explosives, and potentially deter hostile surveillance and unauthorized access. Barriers can be temporary or permanent, natural (e.g., rivers, lakes, waterways, steep terrain, and plants) or manmade (e.g., fencing, walls, bollards, planters, concrete barriers, and fountains). Some properties have effective standoff, while those in urban environments are constrained by space; however, the effective use of barriers can create a secure environment that balances the operational, security, aesthetic, and hospitality interests of the property. Barriers include the following:

Perimeter Barriers

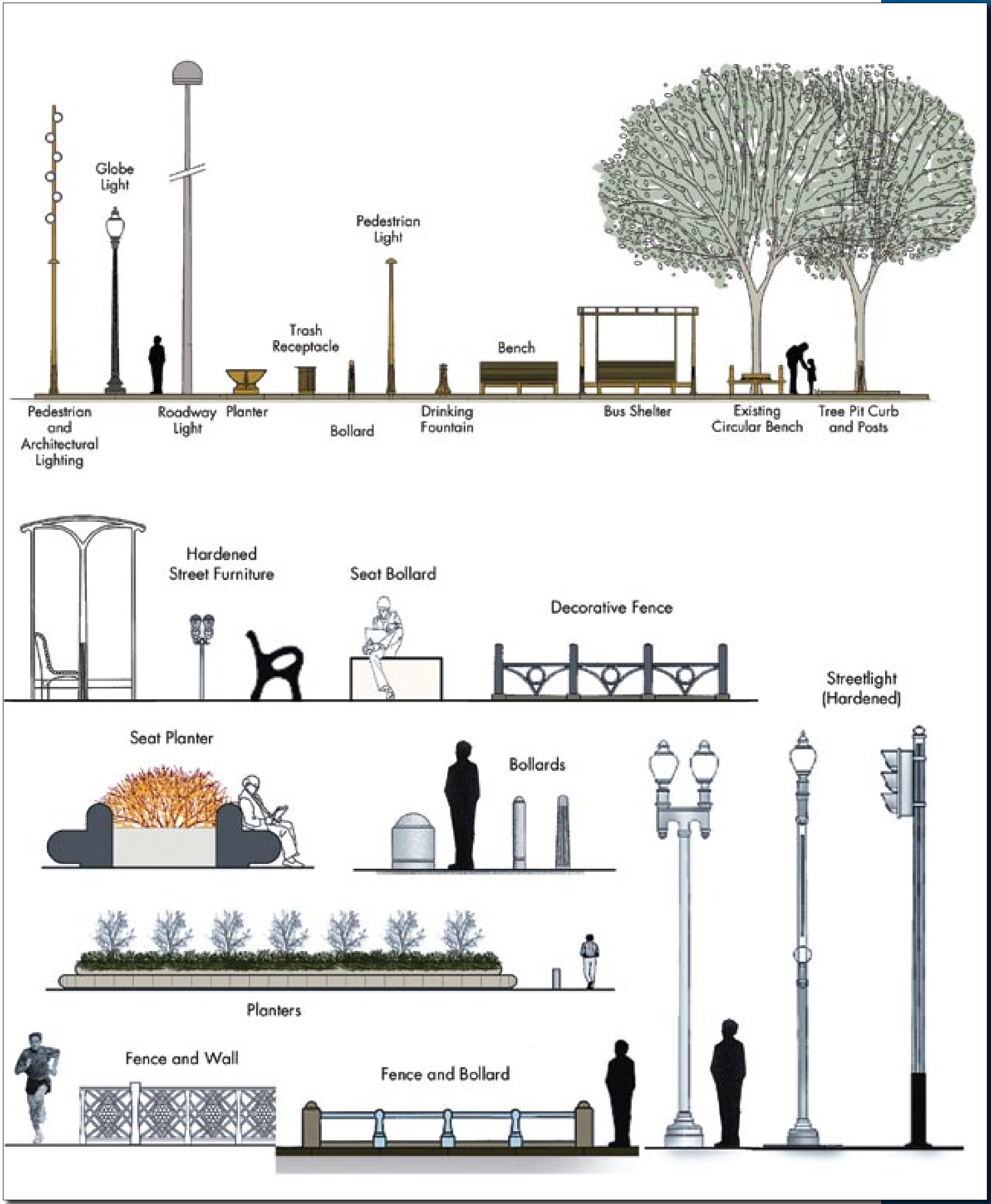
- ❍ Locate the perimeter line, the outermost line that can be protected by security measures, as far as practical from the hotel exterior.
- ❍ Evaluate the need for perimeter barriers around the hotel to clearly demarcate the property line and to deny intrusion, particularly for urban hotels. Consider natural features (e.g., hills, woods, waterways) that could either enhance or inhibit security at the hotel.
- ❍ Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to prevent packages from being hidden and to allow security to observe intruders. Inspect perimeter barriers regularly for gaps, tampering, or indications of intrusion.
- ❍ Consider installing alarms and intrusion-detection equipment at perimeter barriers.
- ❍ If appropriate, install building perimeter barriers (e.g., fences, bollards, decorative flowerpots, high curbs, and shallow ditches) around sensitive or critical buildings in addition to the hotel perimeter barriers. Consider the requirements for fire protection and emergency vehicle access in the design of building perimeter barriers.
- ❍ For a more detailed exploration of how the construction of perimeter barriers can mitigate the risk of terrorist attacks, consult *FEMA 430: Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*, part of the FEMA 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. It is available at http://www.fema.gov/library/viewRecord.do?id=3135.


Risk Management Series
Site and Urban Design for Security
Guidance Against Potential Terrorist Attacks
FEMA 430 / December 2007
FEMA

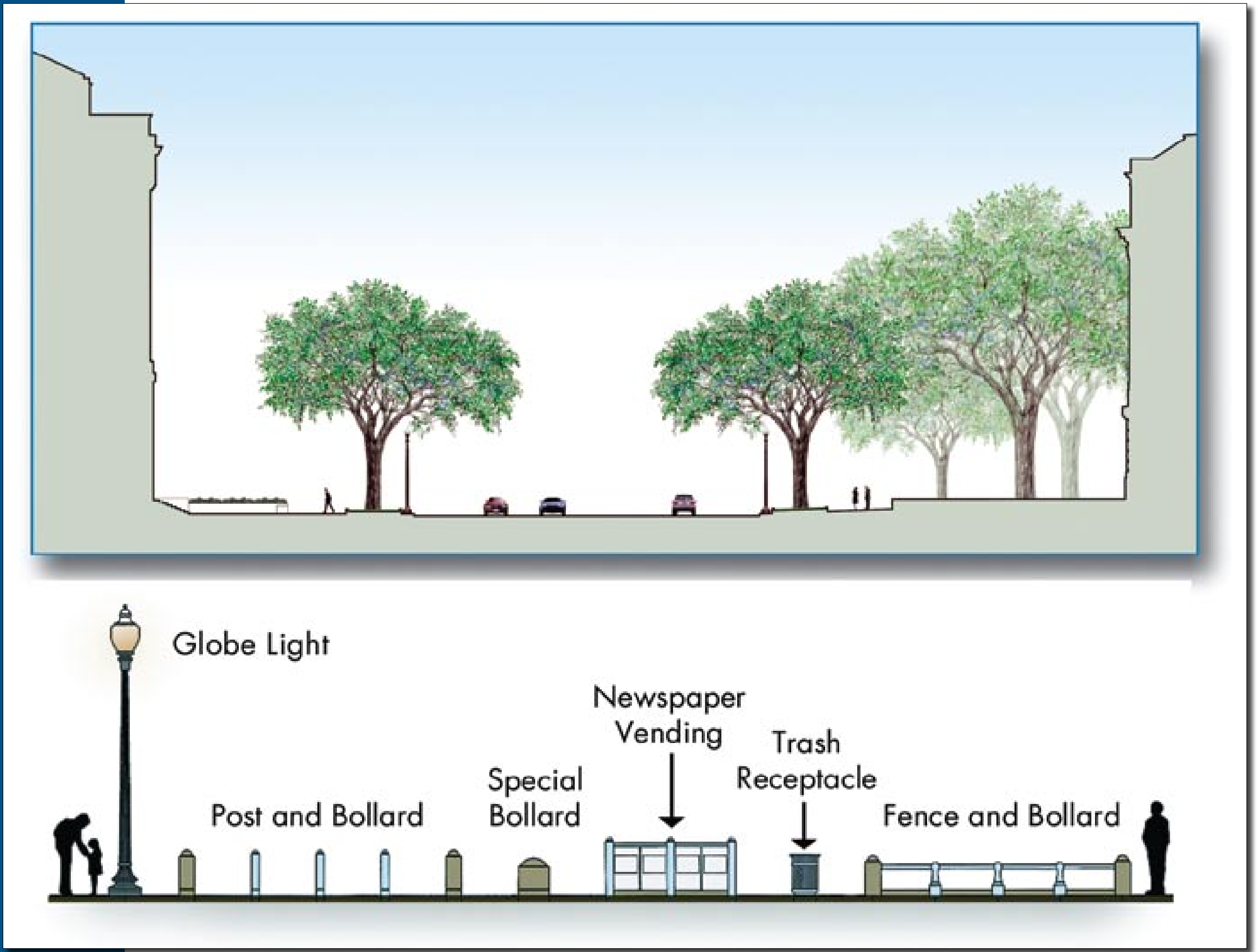
Vehicle Barriers

- ❍ Evaluate vehicle traffic patterns on the hotel grounds. Design and implement traffic control strategies and barriers (e.g., road alignment, serpentine traffic routing, retractable bollards, swing gates, speed bumps, parking control arms, or sliding gates) to control vehicle speed and approaches to the hotel front entrance, and other critical or vulnerable areas of the facility or property.
- ❍ Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from hotel buildings and gathering areas on hotel premises.

- ❍ Evaluate the need for crash-rated vehicle barriers (e.g., bollards, surface mount plate barriers, drum barriers, gate barriers).
- ❍ Install removable bollards on pedestrian walkways to keep unauthorized vehicles off.
- ❍ Consider delay time created by the use of vehicle-control barriers and evaluate for appropriate guest service implications.



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



FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
Streetscape security elements (continued)

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

- ❍ Consider deployment of temporary barriers (e.g., bollards, Jersey barriers, heavy vehicles and equipment, empty containers, trucks loaded with sand) to increase the standoff distances from the hotel, and to control access and traffic flow to the property.
- ❍ Consider implementing the following additional protective measures:
  - Deny access of vehicles onto the premises by stopping them at the property perimeter access point. Deploy redundant barrier controls to enable vehicle screening to be temporarily undertaken at a place of maximum safe distance from the property.
  - Incorporate a secure shuttle service for guest transportation to and from the perimeter vehicle screening point.
  - Incorporate a secure escort process for service deliveries from the perimeter vehicle screening point to the loading dock or drop-off point.

5.6 Communication and Notification

Communications protective measures for a hotel can encompass equipment, protocols, and information sharing, and include the following:

General Measures

- ❍ Develop a communication and notification plan that covers voice, data, and video transfer of information related to security. Consider having prerecorded announcements to play in the event of an emergency. Announcements to be released in the event of an emergency may include weather, natural disasters, false alarms, or other emergencies potentially requiring evacuation or shelter-in-place.

Communications Equipment

- ❍ Install a mass notification system (public address, cell phones, computer override, etc.) that provides a timely means to notify all people at the hotel of threats and give instructions as to responses. Building communications systems should provide real-time notification of occupants and passersby in the immediate vicinity of the hotel during emergency situations.
- ❍ Provide redundant communication channels (e.g., telephone, radio, pager, public address system) that can be used in the event that one channel is disabled. Provide backup electric power (e.g., uninterruptible power supplies, backup generators) to run communications systems.
- ❍ Consider installation of a special panic alarm system in sensitive or critical areas.
- ❍ Consider installation of a priority access communication system to allow access to preferred users involved in emergency management.
- ❍ Test systems regularly and train employees in the use of the various communications systems.
- ❍ Install system(s) that provide communication channels with local law enforcement and emergency responders. Test systems regularly.
- ❍ Have emergency communication equipment (e.g., special cell phones, emergency radios) available for use in the event that all primary communication channels are unavailable.
- ❍ Provide communication security (e.g., encryption, multiple frequencies, countermeasures sweeps) that will prevent unauthorized interception of information being transferred.
- ❍ Train employees not to discuss sensitive information over communications channels that are not secure (e.g., cell phones).
- ❍ Confirm interoperability of communication systems between hotel organizations and local emergency responders. Ensure that all parties can communicate with each other.

❍ Coordinate with communication service providers (e.g., telecommunications companies) on plans and procedures for restoration of service in the event of a disruption.

Communication Protocols

❍ Develop a notification protocol that outlines who should be contacted in emergencies. Designate who is to contact whom within the hotel and with outside organizations. Provide a contact list to all who might need it and keep the list up-to-date. Regularly test the notification protocol through drills and exercises.

❍ Develop a system to account for staff, guests, tenants and contractors. Ensure that the information can be accessed offsite in the event of an emergency. Provide a simple and straightforward means for people to communicate the presence of a potential threat or an emergency (e.g., a hotline number, internal 9-1-1 capability).

❍ Provide guests with information on how to report suspicious people or activities.

❍ Develop a process to warn guests of criminal activity in and around the hotel.

❍ Develop a process for communicating to employees and guests 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 employees who are not on duty.

❍ Consider a contact information checklist to include owners, staff, tenants, law enforcement, other government agencies, hospitals, insurance providers, neighbors, and emergency service contracts. For emergency service contact information checklists, include vendors in charge of electrical, Information Techology (IT), elevators, generators, HAZMAT, heating, Air Conditioning (AC), plumbing, sewage, language translation, etc.

- ❍ Develop a process for communicating with the public and the media regarding security issues, including the handling of inquiries from concerned family and friends. Identify the people who will have responsibility for media interactions. Provide adequate information to the public and media to quell rumors and prevent unnecessary alarm. Take steps to restrict the release of information that might compromise the security posture of the hotel.

Information Sharing

- ❍ Monitor industry and government information on threats, incidents, and response procedures. Report information about the hotel'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, email hsin.helpdesk@dhs.gov.) The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. (See Appendix D: Additional Federal Resources for more information on fusion centers and FBI Joint Terrorism Task Forces).

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

- ❍ Provide a secure means for security staff to communicate with each other during emergencies.
- ❍ Increase frequency of communications with local law enforcement. Advise them of the heightened security status of the hotel. Identify additional security measures that will be implemented.
- ❍ Increase communication 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 working in remote areas and areas isolated from the hotel.
- ❍ Test communication equipment, including primary and backup systems frequently. Have communication backup equipment activated and ready for use in the event of an incident.

5.7 Monitoring, Surveillance, Inspection

General Measures

- ❍ Evaluate needs and design a monitoring, surveillance, and inspection program that is consistent with hotel operations and security requirements. Coordinate with local law enforcement on activities to be undertaken locally, particularly with regard to ensuring awareness of current activities in the area surrounding the hotel.
- ❍ Train security staff to identify counter-surveillance techniques including identifying activities such as suspicious loitering, and taking photos and videos of the hotel.
- ❍ Ensure that routine security patrols include internal and external areas; patrols should not be predictable.

Equipment

- ❍ Install video surveillance equipment (e.g., CCTV, lighting, night-vision equipment) where indicated by a risk assessment. Remember that CCTV is only useful if monitored and used properly. The following practices are helpful when using video surveillance equipment:
  - Provide coverage for the hotel's perimeter, sensitive and critical assets in the hotel, vehicle roadways and parking lots, building entrances, and standoff distances.
  - Provide both centralized and distributed capability to monitor and record video feeds. Maximize the video recording time.

  - Train personnel to interpret video and identify potential security-related events.
  - Review recordings regularly for unusual activities or patterns.
  - Establish procedures to secure video recordings for forensic purposes. If appropriate, provide video feed to local law enforcement and to other organizations outside the hotel.
  - Inspect and test all video equipment regularly, including time and date stamps.
  - Review recordings for unusual activities or patterns when required.

- ❍ Install detector and alarm systems. Include intrusion detectors, fire and smoke alarms, and motion detectors, as appropriate. The following practices are helpful when using detector and alarm systems:
  - Provide both centralized and distributed capability to monitor and record detector and alarm feeds.
  - Train personnel to interpret detector and alarm signals and to identify potential security-related events.
  - Establish procedures to secure detector and alarm recordings for forensic purposes. If appropriate, provide detector and alarm feed to local law enforcement and to other organizations outside the hotel.
  - Inspect and test all equipment regularly.

- ❍ Install and maintain sufficient lighting inside and outside the hotel to assist security personnel when conducting visual assessments during day and nighttime.

- ❍ Ensure mechanical, electrical, gas, power supply, voice/data telecommunications system nodes, security system panels, elevators and critical system panels, and other sensitive rooms are continuously locked, under electronic security, CCTV camera, and intrusion alarm systems surveillance where applicable.

Buildings and Hotel Assets

- ❍ Deploy security staff to regularly inspect hotel perimeter, buildings, parking lots, locker rooms, equipment, trash containers, HVAC systems, and sensitive or critical areas for signs of security issues or breaches. Ensure that the security staff has access to all areas to be inspected.
- ❍ Implement random as well as scheduled inspections; keep patrols regular but unpredictable.
- ❍ Utilize plain clothes, as well as uniformed, patrols. Employ vehicle, foot, and bicycle patrols as appropriate. Pay special attention to assets that are not in frequent use. Train the security staff and other employees to be alert to suspicious items and instruct them on reporting procedures.
- ❍ Maintain an awareness of materials already in place at the facility that could be leveraged for illicit purposes, such as large quantities of flammable materials or dangerous chemicals, and catalog and safeguard these materials accordingly.

People

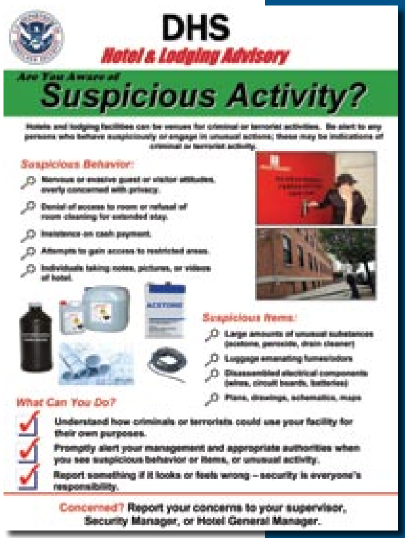
- ❍ Monitor people, including guests, entering and leaving the hotel. Train monitors to detect suspicious behavior (e.g., unusually bulky clothing that might conceal weapons, unusual packages being carried).
- ❍ Monitor the activities of contractors, delivery personnel, and vendors for unusual behavior while they are at the hotel.

Vehicles

- ❍ Monitor all vehicles approaching the hotel for signs of threatening behavior (e.g., unusually high speed). Be prepared to take defensive action against vehicles exhibiting such behavior (e.g., engage barriers, deploy security force vehicles).
- ❍ Consider current and future inspection technologies (e.g., above vehicle and under vehicle surveillance systems, ion scanning, and X-ray equipment).

Luggage, Deliveries, and Mail

- ❍ Monitor and verify deliveries made to the hotel. 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 any deliveries that fail to conform to requirements.
- ❍ Maintain records of all deliveries (e.g., invoices).
- ❍ Inspect all mail for unusual signs (e.g., strange powders, leaking material, no return address). Divert suspicious mail or packages to controlled area for handling. Provide personal protective equipment for those handling suspicious mail or packages.



DHS
Hotel & Lodging Advisory

Are You Aware of
Suspicious Activity?

Hotels and lodging facilities can be venues for criminal or terrorist activities. Be alert to any persons who behave suspiciously or engage in unusual actions; these may be indications of criminal or terrorist activity.

Suspicious Behavior:

- Nervous or evasive guest or visitor attitudes, overly concerned with privacy.
- Denial of access to room or refusal of room cleaning for extended stay.
- Insistence on cash payment.
- Attempts to gain access to restricted areas.
- Individuals taking notes, pictures, or videos of hotel.

Suspicious Items:

- Large amounts of unusual substances (acetone, peroxide, drain cleaner)
- Luggage emanating fumes/odors
- Disassembled electrical components (wires, circuit boards, batteries)
- Plans, drawings, schematics, maps

What Can You Do?

- ✓ Understand how criminals or terrorists could use your facility for their own purposes.
- ✓ Promptly alert your management and appropriate authorities when you see suspicious behavior or items, or unusual activity.
- ✓ Report something if it looks or feels wrong – security is everyone's responsibility.

Concerned? Report your concerns to your supervisor, Security Manager, or Hotel General Manager.

DHS Hotel &
Lodging Advisory Poster

❍ Consider acquiring luggage-screening equipment for use during high-threat and high-profile events.

❍ Ensure all staff is aware of whom to contact if they encounter suspicious activity or suspicious items. Please see Appendix A: *DHS Hotel & Lodging Advisory* Poster for examples of suspicious activity, suspicious items, and what staff can do to increase their awareness.

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

❍ Increase monitoring, surveillance, and inspection of sensitive and critical assets, people, vehicles, materials, and equipment. Reassign staff to assist with surveillance, monitoring, and inspection duties. Request additional support from local law enforcement as necessary.

❍ Increase monitoring of video surveillance, alarms, and detector equipment feeds. Route detector feeds to local law enforcement. Implement continuous monitoring as necessary.

❍ Install additional temporary lighting to illuminate all areas. Leave lighting on 24/7. If possible, increase lighting in buffer zone.

❍ Increase frequency and thoroughness of inspections of hotel buildings and assets to the maximum level sustainable. Close and secure non-essential buildings and assets.

❍ Restrict what people are permitted to carry into the hotel. Screening of baggage may be a significant deterrent. If screening, inspect all luggage brought into the hotel either manually or by deploying portable scanning equipment (e.g., metal detectors, X-ray scanners).

❍ Thoroughly inspect all vehicles that are allowed to enter the hotel. Restrict the number of vehicles permitted to enter to those required to meet essential needs.

❍ Thoroughly inspect all mail and deliveries made to the hotel. Postpone all non-essential deliveries. Process mail and deliveries at a remote site.

❍ Isolate or remove any hazardous materials that might increase the impacts of an attack.

❍ Consider restricting entry to essential personnel only.

5.8 Information Security and Cybersecurity

Confidential business secrets and hotel security information may be of interest to criminals, terrorists and other adversaries, and also can be inadvertently exposed due to natural events or occurrences. Information may be obtained by breaking into hotel information technology (IT) systems, or simply by obtaining it through discarded data. While companies sometimes need to dispose of sensitive information, it is important that employees at all levels understand the role they play in ensuring this information is secure. An IT security breach could severely disrupt or damage a hotel in many ways.

Sensitive information may include staff contact information, brand and product information, customer details, technical specifications, enterprise/business and control systems, and chemical and biological data. Take basic security precautions to prevent sensitive information falling into the wrong hands. The following protective measures could enhance a hotel's security:

- ❍ Restrict access to sensitive hotel data and information (e.g., building plans; business, information technology, mechanical, electrical, fire, life-safety and control systems; and employee directories).
- ❍ Control all sensitive documents by requiring employees to secure them when not in use. Utilize shredders or a document service to destroy unneeded documents.
- ❍ Ensure that copies of security and emergency response plans are protected from unauthorized disclosure.
- ❍ Include security awareness in staff training. Train staff to secure sensitive material, not leave items lying on desktops, and log off computers when not in use.
- ❍ Laptops and portable equipment should be password protected and never left unattended.
- ❍ Restrict usage of computers and equipment with proprietary information to employees on a need-to-know basis.
- ❍ Regularly review publicly available information about the hotel (e.g., the hotel's Web site, social networking sites) to ensure that no sensitive information is provided.
- ❍ Erase or overwrite electronic media (e.g., CD-ROM, DVD, USB flash drives).
- ❍ Invest in secure cabinets to store sensitive material.
- ❍ Keep records of all security-related incidents; review the records regularly to identify patterns and trends.

5.8.1 Cybersecurity

Not only is the protection of physical assets crucial to protecting hotel security, all information kept on hotel computers – customer, company, and financial information – is crucial to business operations, corporate brand and integrity, and customer privacy. If lost, damaged, or stolen, this information may severely impact security and reputation. 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:

General Measures

- ❍ Develop an acceptable use policy for staff regarding personal use of work computers such as Internet use, e-mail, chat rooms, social media, and music download Web sites.
- ❍ Develop and implement a security plan for computer and information system hardware and software. Design and implement secure computer network architecture and ensure that enterprise security policy is followed, including restrictions on user behavior such as application downloads and configuration adjustments.

❍ Develop a recovery and restoration plan to return computer systems to full functionality after an incident. Evaluate the feasibility of manually relocating essential computer equipment in the event of an incident. Identify sources for replacement equipment that your facility can bring into service quickly. Regularly test these plans and procedures.

❍ Back up all of your important information; keep copies in secure, offsite locations.

❍ Regularly test computer security measures (e.g., audits, penetration testing, incident response and recovery plans).

❍ Maintain complete documentation on computer system hardware and software modifications. Require a formal change-management process to track all modifications.

❍ Maintain a well-trained computer security staff with the appropriate knowledge and experience to deal with cybersecurity issues. Conduct more thorough background checks on employees serving as system administrators.

❍ 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. Monitor and review their work when completed.

❍ Provide training to all employees using hotel computer systems on cybersecurity threats (e.g., e-mail phishing, deceptive inquiries from outsiders, malicious code such as viruses, worms, Trojan horse), and measures for protecting the systems. Train employees on their cybersecurity responsibilities (e.g., changing passwords regularly, not divulging computer information to others, not opening unknown e-mail attachments).

❍ Immediately cancel computer access for transferred, retired, or terminated employees. If exit interviews are conducted with employees, ensure this step is part of the exit interview checklist.

❍ 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. Work with Internet service provider to implement protective measures against attacks (e.g., denial-of-service attacks). Stay up-to-date on the latest cyber security threats, incidents, and defensive measures. (Access information provided by the DHS's Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov/cas/signup.html. Additionally, US-CERT encourages reporting on any suspicious activity, including cybersecurity incidents, possible malicious code, vulnerabilities, and phishing related scams at www.us-cert.gov.)

❍ Ensure that your software is updated regularly. Implement any company policies or procedures on preferred software and security standards.

❍ Control physical access to IT facilities (e.g., computer rooms, elevator control panels, boiler rooms, surveillance systems). Install locks and access controls to allow only authorized personnel to enter these facilities. Provide communication capabilities to allow rapid reporting of an unauthorized entry to these facilities.

❍ Control both onsite and offsite electronic access to IT systems by employing passwords, account access restrictions, and other control techniques.

- ○ Develop redundancy in computer hardware and software to permit continued operation of information systems in the event that primary systems are disabled. Backup computer files regularly. Maintain backups in a separate and secure location.
- ○ Thoroughly test all applications that involve the handling of sensitive information to determine their potential vulnerability to compromise.
- ○ Consider using encryption for material that you wish to protect and lock wireless networks. Ensure that wireless networks are designed differently from other hotel, enterprise, or control system networks. This minimizes risk of damage or destruction to wireless capability even if an incident affects other IT systems.
- ○ Establish collaborative relationships with the FBI and other Federal law enforcement agencies involved with computer crimes investigations.

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

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

5.9 Infrastructure Interdependencies

Hotels are complex entities that must rely on partners, providers, and other infrastructure to continue their day-to-day operations. Protective measures should be considered for the following interdependencies:

- ○ Implement quality control inspections on the food supply to hotel restaurants and special events. Conduct background investigations on food suppliers. (For more information on food handling see Section 7, Special Considerations for Adjacent Facilities.)
- ○ Maintain a thorough inventory of all sensitive or critical materials and equipment, and their storage and movement into, out of, and within the hotel.
- ○ Monitor contractor work done at the hotel (e.g., construction, equipment installation, maintenance, cleaning) for unusual activities. Inspect all work before releasing the contractor.

- ❍ Monitor work being done adjacent to the hotel (e.g., road construction, utility equipment servicing) for unusual activities (e.g., someone photographing the hotel or planting packages near the hotel perimeter or assets).
- ❍ Ensure that the hotel has adequate utility service capacity to meet normal and emergency needs. Identify all utility service points that support the hotel. Establish regular communication channels with utility service providers (e.g., electric company, gas company) to 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, in detail, the physical locations of critical support architectures:
  - ■ Communications and information technology
  - ■ Utilities (e.g., facility power, water, air conditioning, etc.)
  - ■ 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 hotel than used for the primary supply equipment, so that no critical node that allows both primary and backup equipment to be affected by a single incident. Inspect and maintain redundant and backup equipment regularly.
- ❍ As much as practical, locate utility supply facilities that are potentially hazardous (e.g., liquid fuel tanks, high-voltage power lines) a safe distance from buildings and areas where large numbers of people congregate.

- ❍ Ensure that employees are familiar with procedures for shutting off utility services (e.g., electricity, natural gas) 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 facility, geographic area, or industry

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

6. Special Considerations for Multiuse Districts & Adjacent Facilities

Recognize that security does not end at a hotel's perimeter. Considering adjacent facilities and the impact they have on a hotel is important. Hotels are often co-located with casinos, malls, airports, convention centers, and ski resorts. These adjacent facilities are usually complementary, but operate with their own distinct security needs, and as such, they require their own protective measures.

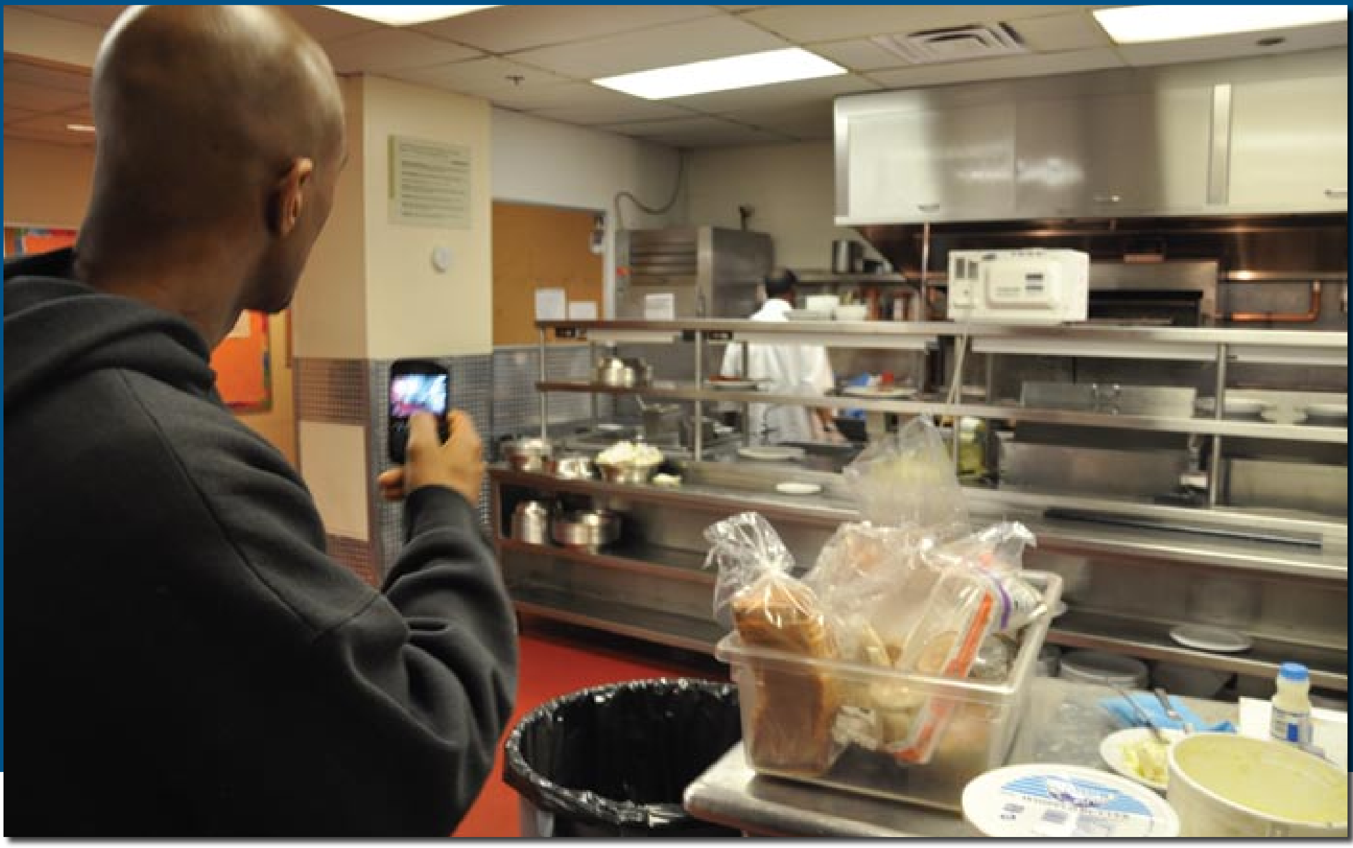
Hotels integrated with other facilities need to consider site- and situation-specific vulnerabilities applicable to both the hotel and the surrounding properties. In the interest of security, it is best to leave aside any tensions between neighbors or landlords/tenants.

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

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

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

7. Special Considerations for Restaurants



As many hotels have restaurants, banquet facilities, and room service capabilities, appropriate procedures should be followed to ensure guest safety. Where restaurants are managed independently from or contracted out by the hotel, hotel officials and restaurant officials should maintain regular communication to coordinate appropriate protective measures and responses. Consider the following nonbinding recommendations from 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*.

Prepare for the possibility of tampering or other malicious, criminal, or terrorist actions:

❍ Conduct an initial assessment of food security procedures and operations; it is recommended that these be kept confidential.

❍ Promote food security awareness to encourage all staff to be alert to any signs of tampering or other malicious, criminal, or terrorist actions; to monitor areas that may be vulnerable to such actions; and to report any findings to identified management (e.g., providing training, instituting a system of rewards, building security into job performance standards).

Investigation of Suspicious Activity

❍ Investigate threats or information about signs of tampering or other malicious, criminal, or terrorist actions. (One available resource is the American Association of Poison Control Centers, found at http://www.aapcc.org/DNN/. Its Poison Help hotline provides immediate access to poison-exposure management instructions and information on potential poisons. Another resource is the FDA's "ALERT Initiative" which identifies five key points that industries and businesses can use to decrease the risk of intentional food contamination at their facility. ALERT is available at http://www.fda.gov/Food/FoodDefense/Training/ALERT/default.htm. For more detail on both resources, see Appendix E: Additional Resources – Web sites).

❍ Alert appropriate law enforcement and public health authorities about any threats of tampering, suspected tampering, or other malicious, criminal, or terrorist actions.

Evaluation Program

❍ Perform random food security inspections of all appropriate areas of the facility, including receiving and warehousing, where applicable, using knowledgeable in-house or third party staff, and keeping this information confidential.

Personal Items

❍ Allow in the establishment only those personal use medicines that are necessary for the health of staff and ensure that these personal use medicines are labeled properly and stored away from stored food and food preparation areas.

❍ Prevent staff from bringing personal items (e.g., lunch containers, purses) into nonpublic food preparation or storage areas.

Training in Food Security Procedures

❍ Incorporate food security awareness, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including seasonal, temporary, contract, and volunteer staff. (The FDA's "Employees FIRST," available at http://www.fda.gov/Food/FoodDefense/Training/ucm135038.htm, is an FDA initiative that food industry managers can include in their ongoing employee food defense training programs. See Appendix E: Additional Resources – Web sites).

Staff Health

❍ Be alert for atypical staff health conditions that staff may voluntarily report and absences that could be an early indicator of tampering or other malicious, criminal, or terrorist actions (i.e., an unusual number of staff who work in the same part of the facility reporting similar symptoms within a short time frame), and report such conditions to local health authorities.

Public

❍ Prevent access to food preparation, storage, and dishwashing areas in the nonpublic areas of the establishment, including loading docks.

Incoming Products

❍ Monitor the serving or display of foods in self-service areas (e.g., salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases).

❍ Use only known and appropriately licensed or permitted, where applicable, sources for all incoming products.

❍ Inform suppliers, distributors, and transporters about FDA's food security guidance, *Food Producers, Processors, and Transporters: Food Secruity Preventive Measures Guidance* and *Importers and Filers: Food Secruity Preventive Measures Guidance*, available at: *http://www.fda.gov/Food/FoodDefense/FoodSecurity/default.htm*.

❍ Take steps to ensure that delivery vehicles are appropriately secured.

❍ Request that transporters have the capability to verify the location of the load at any time, when practical.

❍ Establish delivery schedules. Do not accept unexplained, unscheduled deliveries or drivers, and investigate delayed or missed shipments.

❍ Supervise off-loading of incoming materials, including off hour deliveries.

❍ Reconcile the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt.

❍ Investigate any shipping documents with suspicious alterations.

❍ Inspect incoming products and product returns for signs of tampering, contamination, or damage (e.g., abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or counterfeiting (e.g., inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice).

❍ Reject suspect food.

Storage

❍ Have a system for receiving, storing, and handling distressed, damaged, and returned products, and products left at checkout counters, that minimizes their potential for being compromised (e.g., obtaining the reason for return and requiring proof of identity of the individual returning the product, examining returned or abandoned items for signs of tampering, not reselling returned or abandoned products).

❍ Minimize reuse of containers, shipping packages, cartons, etc., where practical.

8. Special Consideration for Special Events

A special event or a high-profile guest can bring a significant amount of attention to a hotel. This may require special attention to security features at your hotel to ensure proper protection of the event, guests, and of the property in general. Considerations for a hotel hosting a special event or high-profile guest include the following:

- ❍ Examine how everyday operations will be impacted if the hotel or adjacent facilities cater to high-profile guests, government agencies or military, consulates, or controversial guests. Develop a special event checklist or form which notifies all involved departments of the time and impact of a VIP guest or event. For operational security purposes, do not place the VIP guest(s) name on the form.
- ❍ Create a special arrival area for sensitive guests to control traffic flow. Guests may need to arrive well ahead of the event's start time for screening and other security measures. Your set up time may be impacted by these measures. Review current signage on the property and develop new signs for increased traffic flow from pedestrians and vehicles.
- ❍ Implement a policy to allow law enforcement or special security to meet with designated key personnel (such as security and engineering) prior to arrival of the guests or to plan the special events. Provide law enforcement or special security access to the hotel, including arrival/departure areas, parking, room service and restaurants, floor plans, engineering

spaces, roof access, police, fire, rescue, etc. Convey to local law enforcement how your hotel responds to emergency situations such as fire, power loss, elevator malfunction, medical emergencies, and other situations.

❍ Coordinate with local law enforcement or special security services to screen the premises and conduct bomb searches prior to a special event. The hotel may wish to conduct additional staff training and coordinate response procedures with local law enforcement for unattended luggage and suspicious packages during these events.

❍ Anticipate the need for additional security for VIPs or special events if local law enforcement is not providing coverage, or to assist in the confirmation of event attendance lists.

❍ Contact local law enforcement for enhanced security measures including:

- Rerouting traffic at the property;
- Restricting site access; and,
- Securing the perimeter.

❍ Identify employees who may need access to secure areas during a special event, such as engineers, security, housekeeping and catering staff. Security for special events may require the names of these employees for background checks to be conducted in advance of the event, and having this information at hand will decrease the hotel's administrative requirements.

❍ Review with the event host, local law enforcement, additional security, and hotel security the hotel's policy on protesters located on the property as a high-profile guest or event may bring protests or other disruptions to your operations.

❍ Consider how attendance at adjacent facilities such as restaurants or shops that operate within the hotel may influence attendance at the hotel.

❍ For certain high-profile or special events (e.g. national political conventions), DHS, the U.S. Secret Service, or other Federal authorities may be responsible for the planning and orchestration of security measures that entail multijurisdictional responsibilities (i.e. Federal, State, and local authorities). When such an event involves a hotel, the event coordinators will have a number of options and resources available to them, which will include a liaison for the hotel on the security arrangements.

List of Acronyms and Abbreviations

CBR	Chemical, Biological or Radiological
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear and High Yield Explosives
CCEP	Canadian Centre for Emergency Preparedness
CCTV	Closed-circuit television
CDC	Centers for Disease Control and Prevention
CIKR	Critical Infrastructure and Key Resources
COP	Common Operational Picture
CPNI	United Kingdom's Centre for the Protection of National Infrastructure
CSET	Cyber Security Evaluation Tool
DHS	Department of Homeland Security
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
HAZMAT	Hazardous Material
H1N1	Swine Influenza
H5N1	Avian Influenza
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network – Critical Sectors
HVAC	Heating Ventilating and Air Conditioning
iCAV	Integrated Common Analytical Viewer

IED	Improvised Explosive Device
IT	Information Technology
LPE	Limited English Proficiency
NaCTSO	United Kingdom's National Counter Terrorism Security Office
NDMS	National Disaster Medical System
NEMA	National Emergency Management Association
NFPA	National Fire Protection Association
NIPP	National Infrastructure Protection Plan
OPSEC	Operations Security
OSAC	Overseas Security Advisory Council
OSHA	Occupational Safety & Health Administration
PPE	Personal Protective Equipment
PSA	Protective Security Advisor
RFIs/FYIs	Requests for Information/For Your Information
RMS	Risk Management Series
RSS	Really Simple Syndication
RVS	Rapid Visual Screening
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.

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.

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

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.

Aircraft Attack. Terrorists can hijack commercial and general aviation aircraft in order to deliver attackers, explosives, or hazardous materials to an area or facility. The aircraft itself (i.e., September 11th attacks) can also be used as a weapon.

Asset. Person, structure, facility, information, material, or process that has value.

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

Barriers. A means of establishing a controlled access area around a building or asset. Physical barriers can be used to define the physical limits of a building or campus and can help to restrict, channel, or impede access and constitute a continuous obstacle around the site. Physical barriers can create a psychological deterrent for anyone planning an unauthorized entry and they can delay or prevent passage into a site.

Biological Attack. Biological pathogens (i.e., anthrax, tularemia, plague) can cause disease and are attractive to terrorists because of the ability to cause mass casualties and the exhaustion of response resources. Biological agents can be dispersed into the atmosphere via crop-dusting aircraft or other airborne medium; can be introduced into a facility through its HVAC system; or can be spread by contact (i.e., via contaminated letters delivered by mail). A biological attack may involve colorless or odorless agents, and symptoms of exposure may not appear for days or weeks afterwards.

Bomb Threat. Generally defined as a verbal or written threat to detonate an explosive or incendiary device to cause property damage or injuries, whether or not such a device actually exists. Typically delivered by phone, or other telecommunication means, the great majority of such threats are the result of pranks or other sociopathies.

Capability. Means to accomplish a mission, function, or objective.

Chemical Attack. Chemical warfare agents (i.e., sarin or VX) are another weapon of concern. Although not readily available, historically they have been produced and used by terrorists. The most notable instance was the 1995 sarin attack on the Tokyo subway, which killed twelve people.

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

Commercial Facilities Sector-Specific Agency. Recognizing that each CIKR sector possesses its own unique characteristics, operating models, and risk landscapes, Homeland Security Presidential Directive 7 (HSPD-7) designated Federal Government Sector Specific Agencies (SSAs) for each of the CIKR sectors. DHS was designated the SSA for the Commercial Facilities Sector. Within DHS, sector-specific responsibilities have been delegated to the Office of Infrastructure Protection (IP). As the SSA for the Commercial Facilities Sector, IP has the primary responsibility for coordinating with other Federal, State, local, tribal, and private sector partners.

Computer Virus. Malicious code (see Malicious Code) that runs on an infected computer without the knowledge or assistance of the user and makes copies of itself to infect other computers. A virus spreads by infecting a host file and riding with the host wherever it is sent.

Consequence. Effect of an event, incident, or occurrence.

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

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Cyber Attack. Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Information systems can be attacked with the intent of overloading the equipment (i.e., denial-of-service attacks). Information can be altered, stolen, or corrupted to render it unusable.

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 9-1-1 communications systems and control systems.

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

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

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 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.

Emergency Management. As subset of incident management, the coordination and integration of all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other manmade disasters.

Emergency Operations Center. The physical location at 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.

Emergency Plan. The ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

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

Function. Service, process, capability, or operation performed by an asset, system, network, or organization.

Fusion Center. An office staffed with personnel and designed to be an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources.

Hazard. Natural or manmade source or cause of harm or difficulty.

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

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

Improvised Explosive Device (IED). The use of a "homemade" bomb and/or destructive device to destroy, incapacitate, harass, or distract. Because they are improvised, IEDs can come in many forms, ranging from a small pipe bomb to a sophisticated device capable of causing massive damage and loss of life.

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

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.

Intent. Determination to achieve an objective.

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

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.

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 program designed to disrupt the normal operation of a computer by allowing an unauthorized process to occur or by granting unauthorized access.

Manmade Hazards. Acts of terrorism, or any threat, activity, or attack with the element of human intent.

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.

Mitigation. Activities providing a critical foundation in the effort to reduce the loss of life and property from natural and/or manmade disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage. These activities or actions, in most cases, will have a long-term sustained effect.

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

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

Nuclear or Radiological Attack. Weapons-grade nuclear material is very difficult to obtain. However, some sources of radiological materials are more readily available or easily delivered. Radiological materials include radioactive isotopes from a variety of sources, such as medical or industrial equipment. In radiological dispersion devices, often called "dirty bombs," terrorists can attach radiological materials to an explosive to create a wide area of contamination.

Physical Security. Measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media and guidance on how to design structures to resist various hostile acts. Physical security can be as simple as a locked door or as elaborate as multiple layers of armed security guards and guardhouse placement.

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.

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

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.

Resilience. Ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.

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

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

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.

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

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

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 18 CIKR sectors, identified by the criteria set forth in *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.*

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

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.

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

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

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.

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.

TRIPwire Community Gateway. A secure online Web portal designed specifically for the Nation's CIKR 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.

Trojan Horse. A normal-looking file that conceals a dangerous program. Unlike a virus or worm, it does not duplicate itself; it requires the infected file to be executed before it can be run. As a result, Trojan horses are slower to spread than viruses or worms. However, they are extremely dangerous and can cause more harm to a system than a virus or worm.

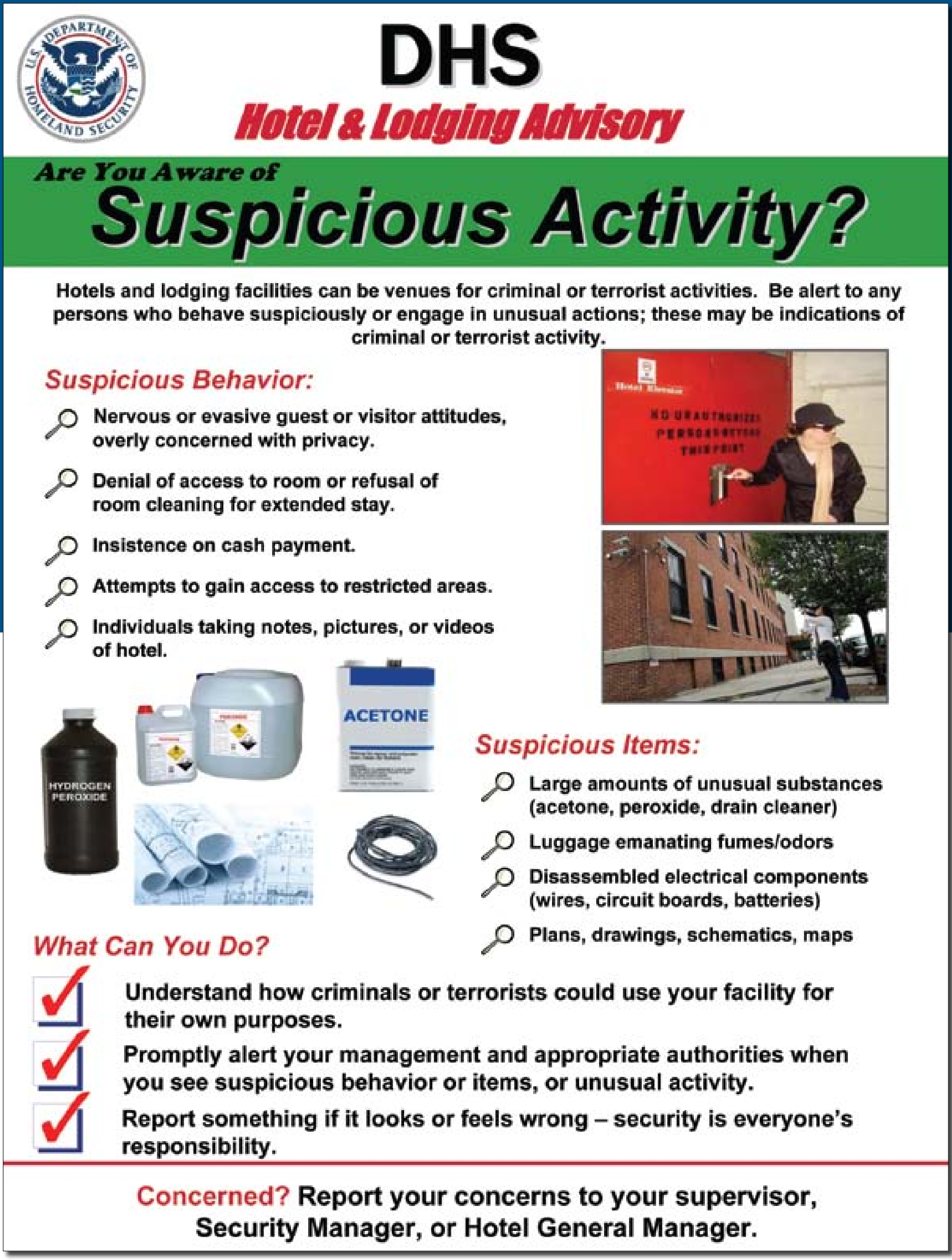
Vehicle-borne IEDs (VBIED). VBIEDs are loaded into a car or truck, or onto a motorcycle. The vehicle can then be parked close to the facility and placed where large numbers of people gather, adjacent to the hotel perimeter, or driven through barriers and then detonated. VBIEDs are much larger and more dangerous than IEDs.

Vulnerability. Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Vulnerability Assessments. Process for identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards.

Worms. A computer worm is malicious code that automatically creates copies of itself. Unlike a virus, it does not require a host to spread. A worm will use the computer network to actively seek out new computers to infect. Some worms use known software vulnerabilities to infect a system. Others, like e-mail worms, trick users into opening them on their system. Worms can be extremely fast moving and destructive.

Appendix A: DHS Hotel & Lodging Advisory Poster



DHS

Hotel & Lodging Advisory

Are You Aware of

Suspicious Activity?

Hotels and lodging facilities can be venues for criminal or terrorist activities. Be alert to any persons who behave suspiciously or engage in unusual actions; these may be indications of criminal or terrorist activity.

Suspicious Behavior:

- Nervous or evasive guest or visitor attitudes, overly concerned with privacy.
- Denial of access to room or refusal of room cleaning for extended stay.
- Insistence on cash payment.
- Attempts to gain access to restricted areas.
- Individuals taking notes, pictures, or videos of hotel.

Suspicious Items:

- Large amounts of unusual substances (acetone, peroxide, drain cleaner)
- Luggage emanating fumes/odors
- Disassembled electrical components (wires, circuit boards, batteries)
- Plans, drawings, schematics, maps

What Can You Do?

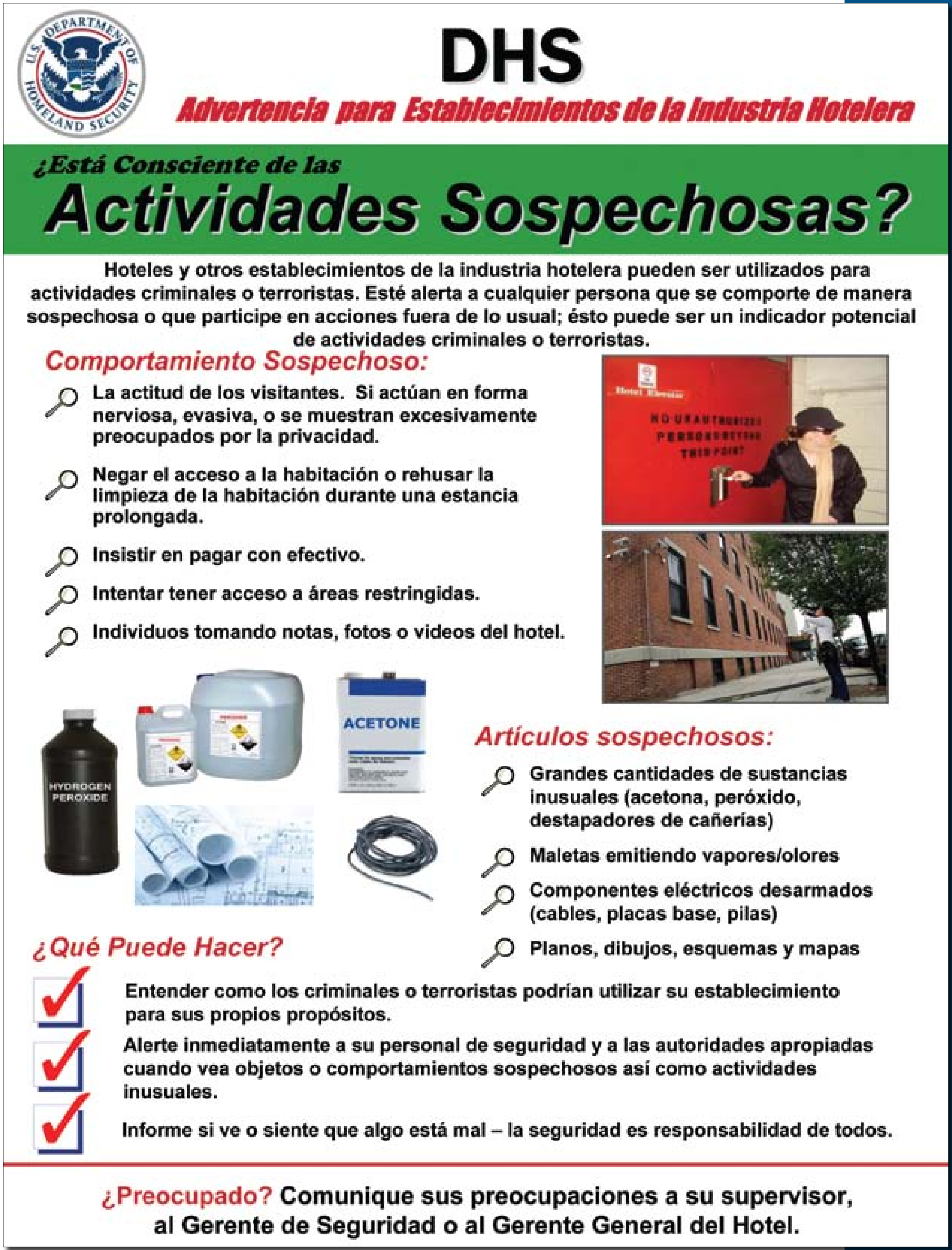
☑ Understand how criminals or terrorists could use your facility for their own purposes.

☑ Promptly alert your management and appropriate authorities when you see suspicious behavior or items, or unusual activity.

☑ Report something if it looks or feels wrong – security is everyone's responsibility.

Concerned? Report your concerns to your supervisor, Security Manager, or Hotel General Manager.

www.dhs.gov/cfsector


HYDROGEN PEROXIDE
ACETONE

DHS

Advertencia para Establecimientos de la Industria Hotelera

¿Está Consciente de las

Actividades Sospechosas?

Hoteles y otros establecimientos de la industria hotelera pueden ser utilizados para actividades criminales o terroristas. Esté alerta a cualquier persona que se comporte de manera sospechosa o que participe en acciones fuera de lo usual; ésto puede ser un indicador potencial de actividades criminales o terroristas.

Comportamiento Sospechoso:

- La actitud de los visitantes. Si actúan en forma nerviosa, evasiva, o se muestran excesivamente preocupados por la privacidad.
- Negar el acceso a la habitación o rehusar la limpieza de la habitación durante una estancia prolongada.
- Insistir en pagar con efectivo.
- Intentar tener acceso a áreas restringidas.
- Individuos tomando notas, fotos o videos del hotel.

Artículos sospechosos:

- Grandes cantidades de sustancias inusuales (acetona, peróxido, destapadores de cañerías)
- Maletas emitiendo vapores/olores
- Componentes eléctricos desarmados (cables, placas base, pilas)
- Planos, dibujos, esquemas y mapas

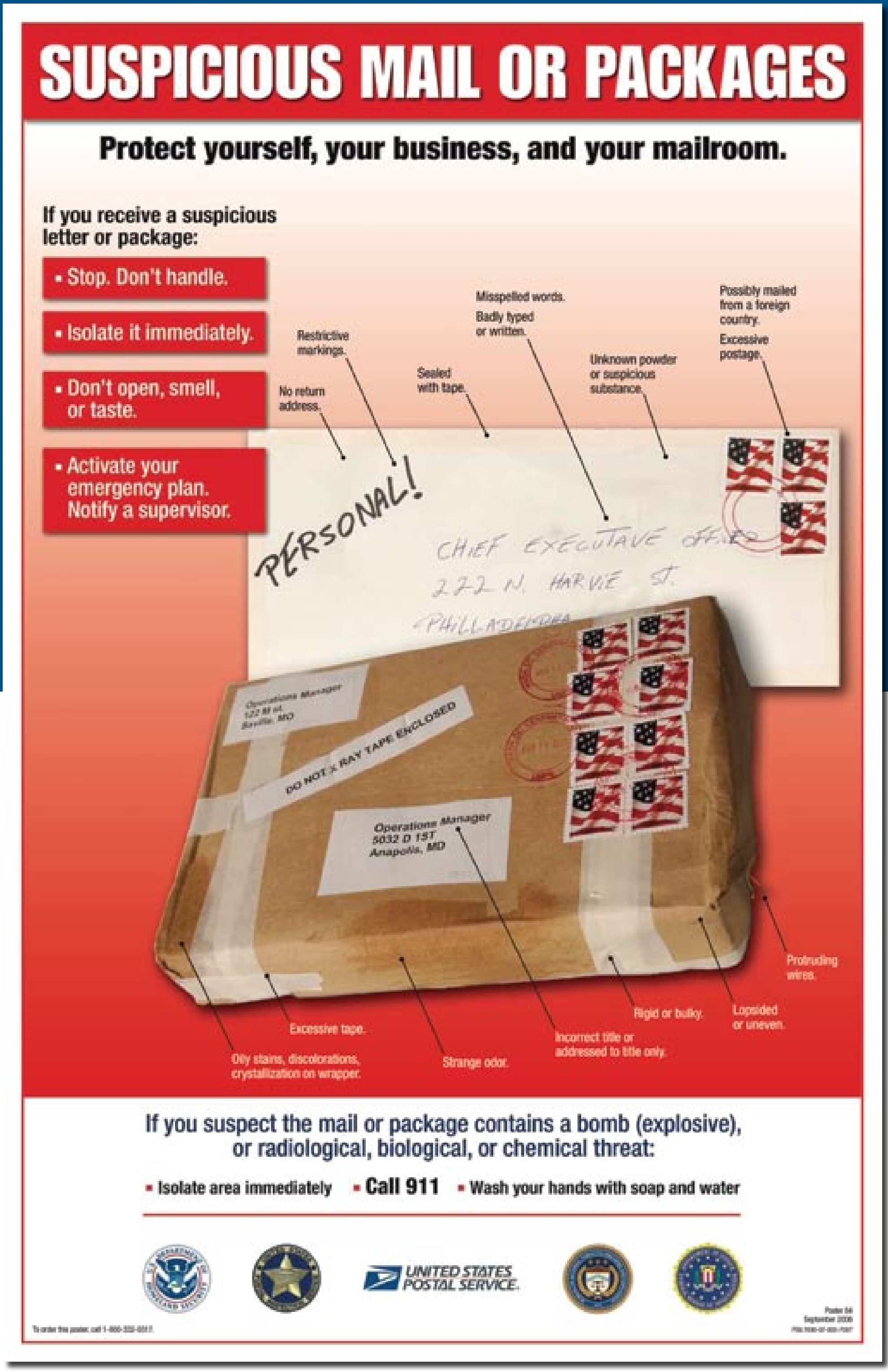
¿Qué Puede Hacer?

- ☑ Entender como los criminales o terroristas podrían utilizar su establecimiento para sus propios propósitos.
- ☑ Alerte inmediatamente a su personal de seguridad y a las autoridades apropiadas cuando vea objetos o comportamientos sospechosos así como actividades inusuales.
- ☑ Informe si ve o siente que algo está mal – la seguridad es responsabilidad de todos.

¿Preocupado? Comunique sus preocupaciones a su supervisor, al Gerente de Seguridad o al Gerente General del Hotel.

www.dhs.gov/cfsector

Appendix B: Suspicious Mail or Packages



SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom.

If you receive a suspicious letter or package:

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

No return address.

Restrictive markings.

Sealed with tape.

Misspelled words.

Badly typed or written.

Unknown powder or suspicious substance.

Possibly mailed from a foreign country.

Excessive postage.

Protruding wires.

Lopsided or uneven.

Rigid or bulky.

Incorrect title or addressed to title only.

Strange odor.

Excessive tape.

Oily stains, discolorations, crystallization on wrapper.

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

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

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

Poster 84
September 2006
PSN 7690-07-000-7087

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

Terrorists may attempt to send chemical, biological or radiological (CBR) materials through the mail. While 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 hotel;
- ❍ 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; and
- ❍ 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; and
- ❍ Strange smell (though some CBR materials are odorless and tasteless).

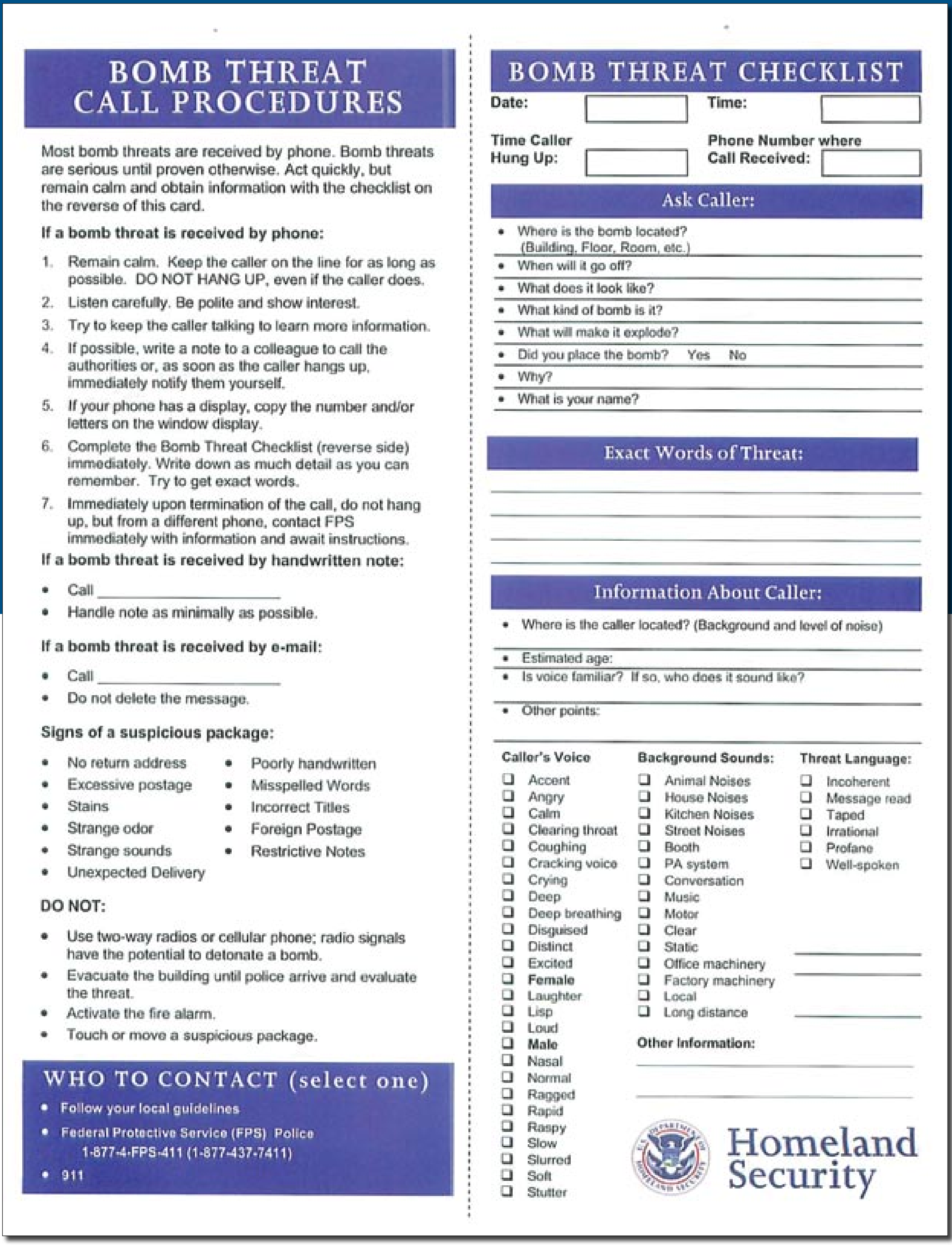
If you receive a suspicious letter or package:

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

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 C: 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

Threat Language:

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

____

____

____

Other Information:

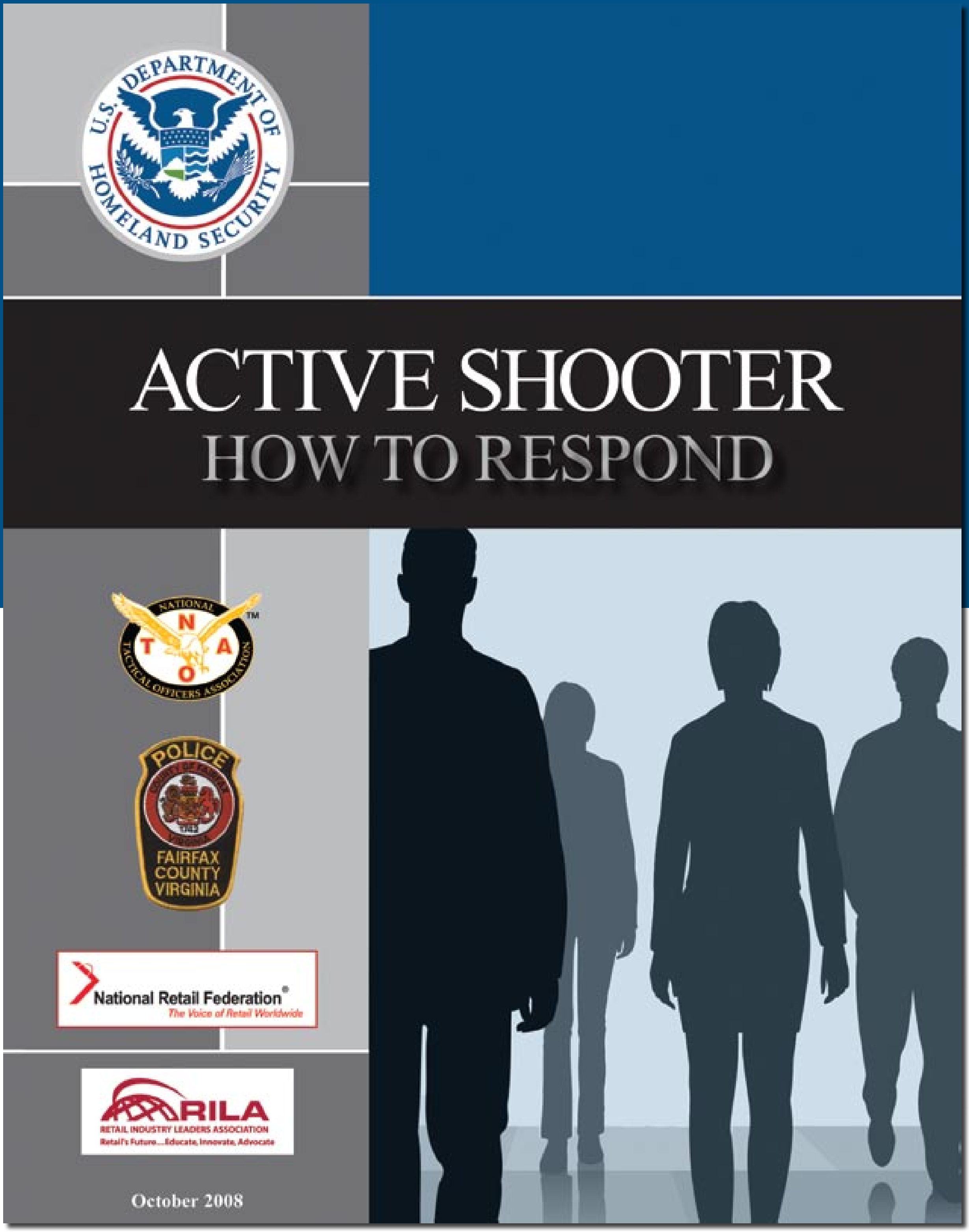
____

____

Homeland Security

DHS Bomb Threat Call Procedures Checklist;
http://www.dhs.gov/xlibrary/assets/ocso-bomb_threat_samepage-brochure.pdf

Appendix D: Additional Federal Resources



ACTIVE SHOOTER
HOW TO RESPOND

U.S. Department of Homeland Security

National Tactical Officers Association

Police County of Fairfax Virginia

National Retail Federation®
The Voice of Retail Worldwide

RILA
Retail Industry Leaders Association
Retail's Future....Educate, Innovate, Advocate

October 2008

DHS *Active Shooter – How To Respond* Booklet;
www.dhs.gov/cfsector

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. The Commercial Facilities Sector maintains an independent site on the HSIN portal, which was designed to allow DHS to share sector-specific threat information with our partners.

Within the Commercial Facilities Sector portal, there is a specific portal for the Lodging Subsector, allowing you to communicate with each other, independent from DHS or other government agencies.

HSIN offers many dynamic capabilities including:

- 24/7 availability
- Document Libraries, including:
  - Active Shooter-How To Respond
  - DHS Hotel & Lodging Advisory Poster
  - *Protective Measures Guide for the U.S. Lodging Industry*
- "HSIN Jabber" instant messaging tool
- Web conferencing
- Incident reporting
- Common Operational Picture (COP) provides situational awareness and analysis
- Integrated Common Analytical Viewer (iCAV) gives geographical visualization
- Announcements
- Discussion Boards
- Task Lists
- Requests For Information/For Your Information (RFIs/FYIs)
- 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, you must 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 Lodging Subsector.

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

TRIPwire Community Gateway

TRIPwire Community Gateway is secure online Web portal designed specifically for the Nation's CIKR 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 CIKR 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

A fusion center is an office staffed with personnel and designed to be an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources.

The role of the fusion center is to compile, blend, analyze, and disseminate criminal intelligence and other information (including but not limited to threat assessments, public safety, law enforcement, public health, social service, and public works information) to support efforts to anticipate, identify, prevent, and monitor criminal activity.

The nearest state and local fusion center's contact information can be found on the Homeland Security Information Network-Critical Sectors (HSIN-CS).

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 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 CIKR;
- ❍ 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: PSAFieldOperationsStaff@hq.dhs.gov.

Vulnerability Assessments

The Department of Homeland Security conducts specialized facility assessments to identify vulnerabilities of CIKR, including assets within the Commercial Facilities Sector and Lodging 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 safeguarding 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.

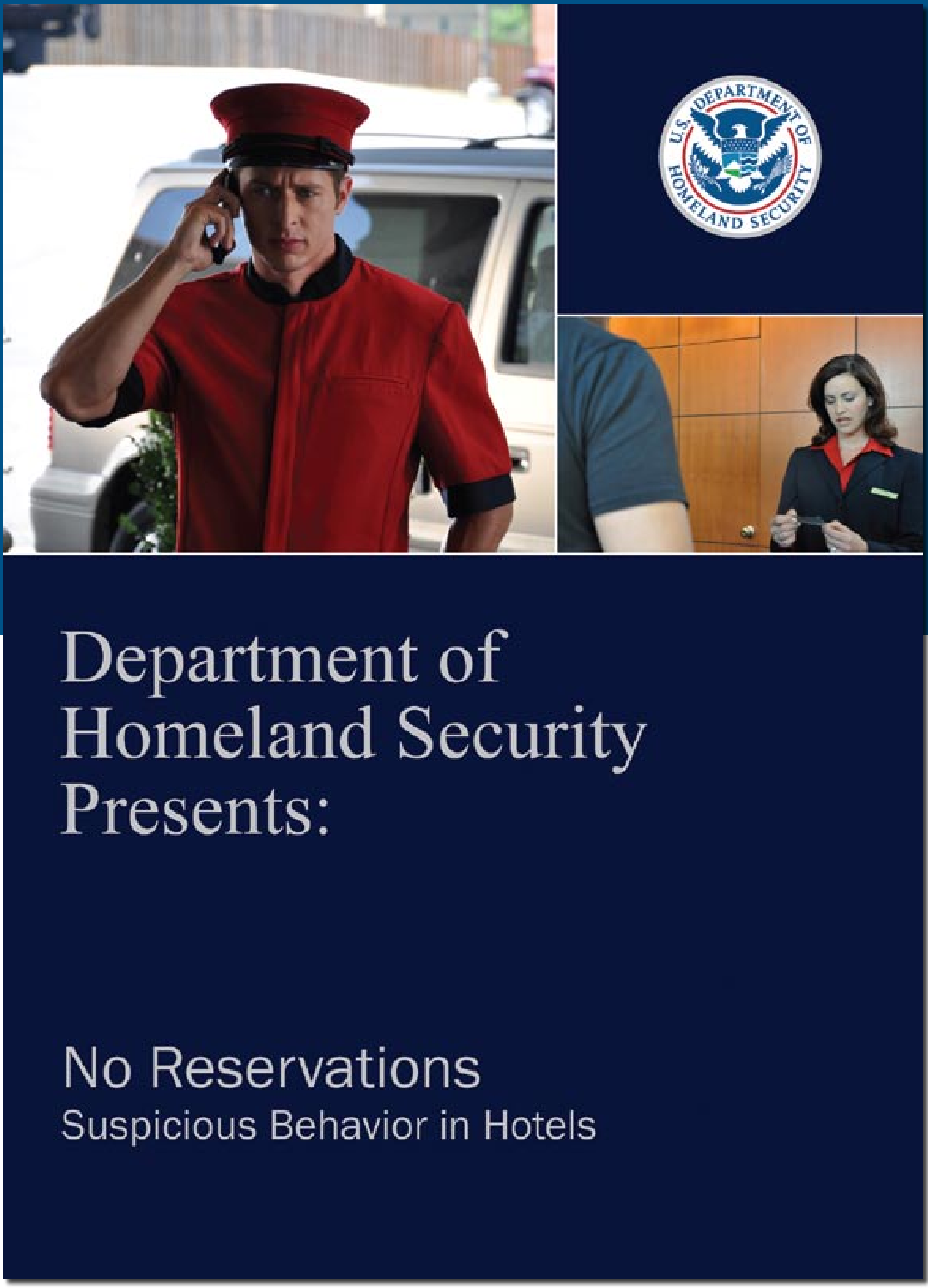
The CSET is a DHS product that assists organizations in protecting these key national cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.

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

Joint Terrorism Task Forces

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

Appendix E: Additional Resources – Web sites



Department of Homeland Security Presents:

No Reservations

Suspicious Behavior in Hotels

No Reservations: Suspicious Behavior in Hotels

www.dhs.gov/cfsector

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

Protecting and ensuring the continuity of the critical infrastructure and key resources (CIKR) 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.
- ❍ *DHS Hotel & Lodging Advisory Poster* (see Appendix A)
- ❍ *No Reservations: Suspicious Behavior in Hotels*. A DHS-produced video designed to raise awareness for hotel 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. http://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. http://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. http://www.ready.gov/business/index.html

U.S. Department of Homeland Security's Computer Emergency Readiness Team

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

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

American Association of Poison Control Centers

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

American Hotel & Lodging Association

Serving the hospitality industry for nearly a century, AH&LA is the sole national association representing all sectors and stakeholders in the lodging industry, including individual hotel property members, hotel companies, student and faculty members, and industry suppliers. *http://www.ahla.com/*

AH&LA has a number of resources available to prevent and manage any potential H1N1 flu outbreak in your lodging business, including *H1N1 Influenza Management in Hotels*. This 26-page lodging industry influenza management guide can assist hotel general managers and other industry professionals in developing their property's H1N1 flu plan, and can be found here: *http://www.ahla.com/flu*

ASIS International

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

ASIS International'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. *http://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

The Centers for Disease Control and Prevention (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. *http://www.cdc.gov/*

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

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

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. http://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/Docs/Pre-employmentscreening.pdf

Centre for the Protection of National Infrastructure – Personnel Security: Threats, Challenges and Measures

This booklet outlines the various activities that constitute a personnel security regime and provides an introductory reference for security managers and human resource managers who are developing or reviewing their approach to personnel security. http://www.cpni.gov.uk/Docs/Pers_Sec_TCM_v2.pdf

Centre for the Protection of National Infrastructure – Protecting Against Terrorism (2nd Edition)

This 38-page booklet gives general protective security advice from the UK's Security Service's (MI5) 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. www.cpni.gov.uk/Docs/Protecting_against_terror_2nd_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/Docs/Risk_Assessment_Pers_Sec_Ed_2.pdf

Centre for the Protection of National Infrastructure – Secure in the Knowledge

This guide is aimed mainly at small and medium-sized businesses. It provides guidance and information to help improve basic security. Ideally it should be read in conjunction with Expecting the Unexpected (see Office for Security and Counter Terrorism – Expecting the

Unexpected below). By following the guidance in both booklets, companies are in the best position to prevent, manage, and recover from a range of threats to their business. http://www.cpni.gov.uk/Docs/Secure_in_the_Knowledge.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/

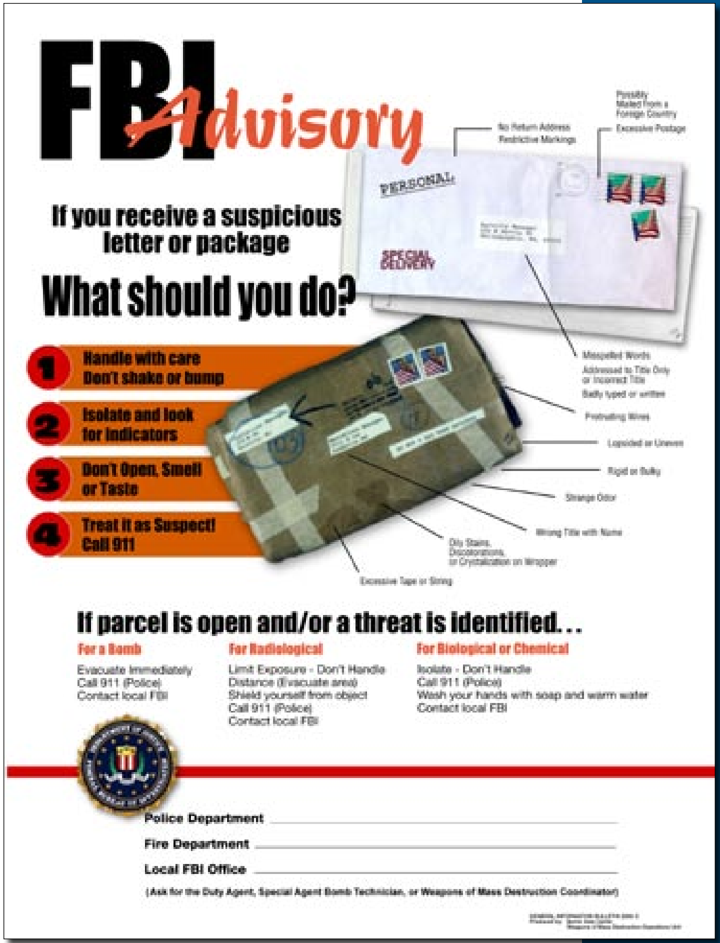
Federal Bureau of Investigation (FBI)

The FBI's mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

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. www.fbi.gov/pressrel/pressrel01/mail3.pdf

Federal Emergency Management Agency (FEMA)

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



FBI Advisory

If you receive a suspicious letter or package

What should you do?

1. Handle with care Don't shake or bump
2. Isolate and look for indicators
3. Don't Open, Smell or Taste
4. Treat it as Suspect! Call 911

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

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

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

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

Police Department ______________________

Fire Department ______________________

Local FBI Office ______________________

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

FBI Advisory Poster; www.fbi.gov/pressrel/pressrel01/mail3.pdf

FEMA Independent Study Program

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

FEMA Security Risk Management Series (RMS) Publications

The following are part of a FEMA series directed at providing design guidance for mitigating multihazard 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 underlying issue is that by improving mitigation and security of high occupancy buildings, we will be better positioned to protect the Nation from potential threats and hazards. The intended audience includes architects and engineers working for private institutions, building owners/operators/managers, and State and local government officials working in the building sciences community.
http://www.fema.gov/plan/prevent/rms/

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

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.
http://www.fema.gov/plan/prevent/rms/rmsp426

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

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.
http://www.fema.gov/library/viewRecord.do?id=3135

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

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

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

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.
http://www.fema.gov/library/viewRecord.do?id=1910

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

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.
http://www.fema.gov/library/viewRecord.do?id=1567

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

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.
http://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.
http://www.fema.gov/library/viewRecord.do?id=3556

Flu.gov

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

The National Counter Terrorism Security Office (NaCTSO) Counter Terrorism Protective Security Advice for Hotels and Restaurants

The National Counter Terrorism Security Office (NaCTSO) is a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). This NaCTSO guide provides protective security advice to those who own, operate, manage, or work in hotels and restaurants. It aids those who are seeking to reduce the risk of a terrorist attack and limit the damage an attack might cause. http://www.nactso.gov.uk/hotelsandrestaurants.php

National Emergency Management Association (NEMA)

National Emergency Management Association (NEMA) is the professional association of and for emergency management directors from all 50 states, eight territories, and the District of Columbia. 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/home.aspx

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. http://www.nfpa.org/catalog/product.asp?title=Code-730-2008-Premises-Security&pid=73008&src=nfpa&order_src=A292

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://security.homeoffice.gov.uk/news-publications/publication-search/guidance/expectingunexpected54ed.html?view=Standard&pubID=689947

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. http://www.osac.gov/

U.S. Army Technical Escort Unit

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

U.S. Department of Health and Human National Disaster Medical System

The National Disaster Medical System (NDMS) is a federally coordinated system that augments the Nation's medical response capability. The overall purpose of the NDMS is to supplement an integrated national medical response capability for assisting State and local authorities in 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.
http://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.
http://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.
http://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.
http://www.fda.gov/Food/FoodDefense/Training/ucm135038.htm

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.
http://www.osha.gov

U.S. Postal Service

This PDF presentation from the U.S. Postal Service outlines the basic identification of a suspicious package and the actions that should be taken if personnel encounter such a package.
http://www.usps.com/communications/news/security/suspiciousmail.htm