



Homeland Security Advisory System (HSAS) Commercial Facilities Sector Guidance Template

Purpose: The Department of Homeland Security (DHS) is committed to working with the 18 CIKR sectors to improve its understanding of the effects on businesses when the HSAS threat level is changed. Over the coming months, DHS will work with the Sector Coordinating Councils (SCCs), the Sector-Specific Agencies (SSAs), and other Sector Partnership stakeholders to catalogue actions taken by each sector when the threat level is changed to either Orange or Red. Gathering and updating this information improves DHS' ability to target its threat level declarations, tailoring the changes to account for variations to the risk profile for each respective sector. Furthermore, this project provides transparency to both government and industry regarding the operational environment when the national threat level changes.

How to Use Guidance Template: This guidance template serves as a non-prescriptive reference for commercial facility owner-operators to use to capture and refine new or existing sector actions taken when the threat level changes. Most sectors already possess guidelines recommending actions to be taken in the event the threat level changes. This project seeks to update or harmonize existing work wherever possible, rather than duplicating previous coordination between DHS and the commercial facilities sector. However, this template presents one way of organizing and gathering sector actions for those sectors seeking to either create new actions or update existing processes. This guidance template addresses some of the major challenges the sectors may face and should consider addressing in their respective actions within the seven key areas highlighted by yellow boxes in the Guidance sections.

Considerations:

These considerations are designed to stimulate thinking about a facility's further actions and options in response to a threat level change within the Commercial Facilities Sector. The Sector consists of eight diverse subsectors, including Public Assembly, Sports Leagues, Resorts, Lodging, Outdoor Events, Entertainment and Media, Real Estate, and Retail. The majority of the facilities are owned and operated by private companies, and the public may move freely through these "open public access" facilities. For the most part, facility owners and operators are responsible for assessing their facility's specific vulnerabilities and practicing prudent risk management and mitigation measures. Their responses to a threat level change are unique to their individual facility type and within each subsector.

Planning Assumptions: A recent document produced by DHS' Protective Security Coordination Division found that the private sector made four key assumptions regarding elevated threat levels. They are:

- The duration of an elevated threat status (Orange, Red) will be finite and short-lived. Time at the Orange threat level will be measured in weeks and not months, and at the Red level in days and not weeks. This assumption often drives the complexity of recommended measures.
- Industry decisions to implement protective measures will continue to depend on the government's ability to articulate threats with a high level of specificity (i.e., a threat to a sector component or geographic area). This specificity will allow threatened sectors to tailor protective measures to a sector component or region, depending upon the nature of the threat.
- Additional human security assets will be readily available when the threat level is increased. Recommendations exist that suggest additional checkpoints, guards, patrols, inspections, and even National Guard troops be put in place when the threat level is increased.
- Mechanisms and channels for communicating threat information exist for each sector and are utilized by DHS.



PLANNING AND PREPAREDNESS



Considerations

Baseline Countermeasures (HSAS YELLOW)

- ◆ Designate a security coordinator to develop, implement, and coordinate all security-related activities. Previous security experience is highly preferable.
- ◆ Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits on a regular and continuing basis. Include assessments of other activities and operations in the vicinity (e.g., airports, chemical plants, government buildings, pipelines, rail lines) to determine if there is any potential for them to increase security risks to the commercial facility. On the basis of these analyses, develop a comprehensive security plan and emergency response plan for the commercial facility. Include (these should be in bullets): standard operating procedures (SOPs) to cover all potential emergency situations, including procedures for dealing with multiple events (e.g., explosives attack and loss of electric power); an identification of security responsibilities and a chain-of-command for responding to an incident; Operations Security (OPSEC) procedures to cover routine security activities by all employees; and, procedures for dealing with people who have special needs (e.g., physical disabilities, non-English-speaking).
- ◆ Establish, if applicable (depending on facility type, size, and location), liaison and regular communication with local law enforcement and emergency responders, State and Federal law enforcement and terrorism agencies, public health organizations, and industry organizations to enhance information exchange, clarify emergency responses, track threat conditions, and support investigations. The facility's security and emergency response plans should be coordinated with appropriate agencies and should include mutual aid agreements. Critical information about the facility (e.g., floor plans, location of emergency equipment, notification and contact lists) should be shared with local law enforcement and emergency responders.
- ◆ Keep copies of the security and emergency response plans in redundant locations. Ensure that the plans are protected from unauthorized disclosure.
- ◆ Involve employees at several levels in security planning. Use third-party evaluations and verification of the plans.
- ◆ Restrict access to sensitive facility data and information (e.g., facility building plans, mechanical, electrical, gas, water, fire, and life safety systems).
- ◆ Ensure, if practical, that one or more facility employees, including a senior security official, who are familiar with the plans are available for deployment at all times. Maintain contact lists of persons to contact in an emergency.
- ◆ Conduct regular exercises with facility employees (and tenants if applicable) to test the security and emergency response plans and to ensure that adequate resources are available to implement the plans and that all facility operating units can implement their responsibilities under the plans. Also, conduct regular exercises with law enforcement and emergency responders to familiarize them with the facility and its security and emergency procedures.



- ◆ Establish, if practical, the capability to collect and interpret available threat intelligence from local, State, and Federal 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.
- ◆ Keep records of all security-related incidents. Review regularly to identify patterns and trends.
- ◆ Establish procedures for facility evacuation and for shelter-in-place situations. For shelter-in-place situation, ensure that a facility is available this is adequately stocked with food, water, and supplies to accommodate the number of people who might need to use it.
- ◆ Develop policies and procedures for dealing with hoaxes and false alarms so that these would not unduly burden facility operations.
- ◆ Develop policies and procedures for dealing with the media and the public in the event of an incident to advise them of the situation and to diffuse rumors and panic.
- ◆ Install an emergency operations center or emergency command center that can be used to coordinate resources during an incident. If necessary, also consider a backup center for use in the event the primary center is disabled.
- ◆ Develop procedures for shutting down the facility if the threat is deemed too serious to continue operations.
- ◆ Control all sensitive documents by requiring employees to secure them when not in use. Utilize shredders or a document service to destroy unneeded documents.
- ◆ Incorporate security awareness and appropriate response procedures for security situations into employee training programs conducted for employees (and tenants if applicable).
- ◆ Procedures to provide for the safety of employees during a security incident.

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Review and implement actions specified in the security and emergency response plans; adjust the plans as necessary to deal with specific threat information.
- ◆ Ensure that the facility has smoke-proof stairways and exit corridors that can be used for evacuation.



- ◆ Activate the emergency operations center, as appropriate.
- ◆ Test all communications devices and networks to ensure they are operational and then do so on a regular basis to verify their continued operation.
- ◆ Review policies and procedures for dealing with the media and public in the event of an emergency to advise them of the situation and diffuse rumors and panic.
- ◆ Protect communication and information technology (IT) centers.
- ◆ Evaluate need to shelter-in-place and/or evacuate.
- ◆ Communicate as necessary within the facility and within the community.
- ◆ Move objects that could become projectiles (e.g., trash containers, crates, loose items not attached to a building or to the ground) a safe distance from buildings and areas where large numbers of people congregate.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (**HSAS ORANGE**) measures listed above.
- ◆ Ensure all High Alert (HSAS Orange) measures listed above are implemented.
- ◆ Review available threat information and determine if additional special protective measures are needed (i.e., evacuate the facility, or close the facility).
- ◆ Evaluate the need to isolate or shut down communication and IT networks
- ◆ Ensure unauthorized personnel are not in the facility or critical areas.



PERSONNEL

Considerations

Baseline Countermeasures (HSAS YELLOW)

- ◆ Conduct a background check on all employees. 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.
- ◆ Incorporate security awareness and appropriate response procedures for security situation into employee training programs. Include the following in the training (these should be in bullets): SOPs in the security and emergency response plans that are used for different types of incidents; maintaining alertness to and recognizing situations that may pose a security threat (e.g., suspicious person, persons without proper employee identification, persons carrying unusual packages, unattended vehicles and packages, strange odors or liquids); contact and notification protocols for suspicious situations and emergencies; caution in providing facility information to outsiders; and, procedures to provide for the safety of employees during a security incident.
- ◆ Maintain up-to-date security training with regular refresher courses. Maintain records of employee training that has been completed.
- ◆ Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., irregular work hours, attempts to access unauthorized areas or systems, patterns of employee illness that might indicate exposure to a toxic agent). Maintain awareness of any unusual patterns of employee illness that might indicate exposure to a toxic agent.
- ◆ Provide additional security measures (e.g., bodyguards) for high-profile and critical employees and guests.
- ◆ Determine the need for personal protective equipment for employees (e.g., toxic material detectors, breathing apparatus). Deploy equipment for ready use in the event of an incident.
- ◆ Review the personnel files of recently terminated employees to determine if they pose a security risk. Take appropriate actions to mitigate the risk.
- ◆ Provide security information and training to all non-employees visiting the facility. 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 facility.
- ◆ If applicable, check guest identification upon check-in.
- ◆ If applicable, provide guests with information on how to report suspicious people or activities.



Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Communicate as necessary within the facility, the associated structures, and within the community.
- ◆ Remind personnel of their role in emergency response and post attack recovery plans.
- ◆ Provide additional training and reminders to employees about the security situation. Provide refreshers on SOPs to be used for different types of incidents.
- ◆ Have employees vary their routines to avoid predictability.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.
- ◆ Ensure all High Alert (HSAS Orange) measures listed above are implemented.



SECURITY FORCE

Considerations

Baseline Countermeasures (HSAS **YELLOW**)

- ◆ Maintain an adequately sized, equipped, and trained security force. Ensure that adequate security personnel are on duty or on call in the event of an incident. Determine the availability of security force reinforcements that would be deployed during heightened threat conditions. Conduct more rigorous background checks on security force personnel.
- ◆ Coordinate security force operations with local law enforcement and, as needed, with State and Federal agencies.
- ◆ Develop a procedure and location for detaining and questioning persons displaying suspicious behavior and/or violating security regulations. Train security force personnel in appropriate methods for dealing with these people.
- ◆ Conduct regular drills and exercises with security force. Involve local law enforcement and other agencies as appropriate.
- ◆ Alter the appearance of security force personnel (e.g., change uniforms or vests, wear plain clothes) to disrupt terrorist planning.
- ◆ Develop a security force patrol schedule that includes both regular and random stops and timing.
- ◆ Provide security information and training to all nonemployees who visit the facility.
- ◆ Require contractors, vendors, and temporary employment agencies to vouch for the background and security of their personnel who will visit the facility and make available for audit.
- ◆ Provide, if applicable, personal protective equipment (e.g., respirators, body armor) to security force personnel as appropriate.

Protective Measures during Periods of High Alert (HSAS **ORANGE**)

- ◆ Ensure you have implemented all Baseline Countermeasures (**HSAS YELLOW**) listed above.
- ◆ Increase security force presence by using overtime and/or additional personnel. Increase frequency of patrols. Increase patrols and inspection of unstaffed and remote parts of the facility.
- ◆ Extend patrols to a wider perimeter around the facility in coordination with local law enforcement.
- ◆ Activate a security command post (e.g., within the emergency operations center).
- ◆ Increase security staff to add surveillance or act as a deterrent and prevent unauthorized access to secure areas.



- ◆ Arrange for and deploy plain-clothes law enforcement or security officials for surveillance as appropriate.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.
- ◆ Ensure all High Alert (HSAS Orange) measures listed above are implemented.
- ◆ Increase the security force presence to the maximum level sustainable.
- ◆ Request additional security force support from law enforcement.
- ◆ Increase or redirect personnel to address critical emergency needs.
- ◆ Increase perimeter and buffer zone patrols and inspections of the facility.
- ◆ Ensure guard forces are prepared for evacuating or sheltering-in-place.
- ◆ Coordinate with local authorities regarding closing of public roads and facilities.
- ◆ Staff all critical access points and restricted areas on a 24/7 basis.



ACCESS CONTROL

Considerations

Baseline Countermeasures (HSAS YELLOW)

- ◆ Define the facility perimeter and areas within the facility that require access control for tenants (if applicable), visitors, contractors, and vehicles. Identify especially sensitive or critical areas (e.g., control rooms, communication centers, shipping areas, mailrooms, fuel or chemical storage tanks, pipelines and valves, HVAC and other utility service areas) that require special access controls. Maintain facility access points to the minimum needed consistent with facility operational requirements and safety considerations. 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 building. Evaluate and select access control measures for each access point.
- ◆ Identify a buffer zone that extends out from the boundary that can be used to further restrict access to the facility when necessary. Coordinate, if practical, with local law enforcement on measures to be used in the buffer zone.
- ◆ Provide appropriate signage to identify access points and areas with restricted access.
- ◆ Provide security guards at key access points. Train guards to identify pedestrians, vehicles, and water vessels that are permitted access. Train guards on procedures for denying access.
- ◆ Prohibit entry of security-sensitive items (e.g., firearms, explosives, illegal drugs). Train security force to identify and confiscate such items.
- ◆ Strictly enforce all access control measures (e.g., employee badge check, locking of buildings not in use) on a continuing basis. Allow no exceptions.
- ◆ Under special circumstances, determine the need for establishing restricted air space to prohibit aircraft flying over high-rise and high-occupancy residential buildings. Coordinate with local and Federal aviation officials about implementing and enforcing these restrictions.
- ◆ Issue photo identification (ID) badges to all employees. Require that badges be displayed and verified to gain access to the facility. Occasionally test the response of employees to unbadged persons at the facility. Require that employee badges be worn at all times in the facility. As necessary, issue special employee badges to authorize access to sensitive areas. Utilize electronic access tracking system to log entry and exit from the hotel and/or sensitive areas.
- ◆ Collect employee ID, keys, and other company property when the person is no longer employed. Consider changing locks.
- ◆ Issue special ID badges to contractors, cleaning crews, vendors, and temporary employees. Require that badges be



displayed and verified to gain access to the building.

- ◆ Require that badges be worn at all times in the facility. Collect all badges when visit is complete.
- ◆ Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees. Require that the badges be displayed and verified to gain access to the facility. Require that badges be worn at all times in the facility. Collect all badges when visit is complete.
- ◆ Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement. Require sign-in and sign-out of contractors, vendors, and temporary employees.
- ◆ Encourage employees to become familiar with contractors, vendors, and temporary employees. Ask them to question any unusual or unrecognized people and report incidents to facility security personnel.
- ◆ Escort all nonemployees in sensitive or critical areas.
- ◆ If event registration is required, consider the following actions for conventioners: supply relevant security guidelines and emergency plans, request contact information in case of emergency, and request photo identification at event check-in.
- ◆ Have security personnel deny access to anyone displaying suspicious behavior.
- ◆ Use centralized parking and shuttle service to keep vehicles away from critical assets.
- ◆ Maintain a database of employee-owned vehicles; issue parking permits for designated areas.
- ◆ Review vehicle traffic patterns inside the facility grounds. To the extent possible, keep vehicles away from sensitive or critical assets and from areas where large numbers of people congregate.
- ◆ Review all requests for visitor access, tours, and demonstrations and displays (e.g., open house). If possible, screen visitor requests with local law enforcement to identify potential problems.
- ◆ Require visitors to sign in and sign out. Issue special ID badges to visitors. Require that badges be displayed and verified to gain access to the facility. Require that badges be worn at all times in the facility. Collect all badges when visit is complete.
- ◆ Limit access to visitors, patrons, or customers to a level consistent with facility operations. Have security personnel deny access to anyone displaying suspicious behavior.
- ◆ Where possible, maintain a list of regular customers, vendors, delivery personnel, and other regular visitors.
- ◆ Use a centralized parking and shuttle service to keep vehicles away from critical assets.



- ◆ Maintain a database of employee-owned vehicles. Issue parking permits for designated areas.
- ◆ Positively identify all vehicles and drivers that enter the facility. Deny access to suspicious vehicles (e.g., with leaking fluids, apparently heavily overloaded, with unusual odors) and to vehicles and drivers with improper documentation (e.g., cargo manifest) or refusing to provide identification and/or to submit to inspection.
- ◆ Review vehicle traffic patterns inside the building parking areas. To the extent possible, keep vehicles distant 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.
- ◆ Approach all illegally parked vehicles. Require that they be moved or have them towed.
- ◆ Lock all facility owned vehicles and park them in a secure area when not in use. Provide additional security for the facility's emergency response.
- ◆ Identify all vehicles and drivers that enter the building. Maintain log of all nontenants and nonemployee vehicles entering the facility. Deny access to suspicious vehicles (e.g., with leaking fluids, apparently heavily overloaded, with unusual odors) and to delivery vehicles and drivers with improper documentation (e.g., cargo manifest) or refusing to provide identification and/or to submit to inspection.
- ◆ Review vehicle traffic patterns inside the facility. To the extent possible, keep vehicles distant from restricted areas.
- ◆ Regularly inspect and test all access control devices.
- ◆ Train mailroom and receiving personnel to recognize suspicious mail, packages, shipments, or deliveries and in procedures to follow.
- ◆ Provide security measures (e.g., alarms, door and window locks, barred entryways, fencing and gate locks, times closure devices) to buildings, rooms, elevators, shipping/receiving areas, utility access points (e.g., manholes, HVAC systems), hazardous materials (e.g., fuels, chemicals), and other areas with restricted access. Use higher security controls (e.g., card swipe locks, biometric identification) in sensitive or critical areas. Maintain an audit trail of those accessing these areas.
- ◆ Install and regularly test electronic access control systems and intrusion detection systems for nonpublic critical areas in a shopping mall.
- ◆ Provide additional security to buildings and other assets that are on the facility perimeter where they may be more open to attempts to unauthorized entry.



- ◆ Provide security ladders, awnings, and parapets that give access to building roofs, HVAC systems, and other critical equipment. Ensure that nearby foliage (e.g., trees, shrubs) cannot be used to gain access to roofs of buildings.
- ◆ Lock and secure all buildings and other assets when not in use. Ensure that all areas containing equipment used by the security force (e.g., communications gear, uniforms, weapons) are locked and secured.
- ◆ Implement rigorous key control procedures. Track holders of all keys. Secure master keys. Require that terminated employees and contractors completing their work return all keys.
- ◆ Secure all tools that could be used to force entry into a secured area, building, or room (e.g., bolt cutter, hacksaws, cutting torches).
- ◆ Restrict storage of luggage to locations away from areas where large numbers of people congregate.
- ◆ Establish a process for controlling access and egress to the facility, including designated, monitored points of entry.
- ◆ Establish a buffer zone and perimeter around the facility and a process for controlling access and egress through a buffer zone perimeter, if necessary.
- ◆ Maintain building/structure perimeter so that it is free from trees, branches, and telephone poles that could provide access to the facility's upper floors/levels or roof, if applicable.
- ◆ Ensure that high-risk areas, such as locker rooms, weight rooms, etc., are protected by high-security locks and an alarm system.
- ◆ Identify, secure, and control access to all utility services to the facility. Limit and control access to all crawl spaces, utility tunnels, and other means of under-building access to prevent the planting of explosives.

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (**HSAS YELLOW**) listed above.
- ◆ Reduce the number of access points for pedestrians, vehicles, patrons, tenants, visitors, and customers. Increase the security (e.g., additional guards, inspections) at each open access point.
- ◆ Restrict parking to areas away from critical assets. Evaluate the closure of underground or under-building parking lots.
- ◆ Accept deliveries only during daytime hours and away from critical facilities.
- ◆ Restrict access by nonemployees (e.g., contractors, vendors, visitors) to only those needed to support critical activities in



facilities that can still function without open access to the public, such as commercial office buildings. Delay all nonessential contractor work. Escort all nonemployees while at the building. In facilities that rely on visitors to function (e.g., convention centers, stadiums, amusement parks, and shopping malls) increase monitoring, surveillance, and inspection measures, as well as other measures.

- ◆ Search vehicles that enter the facility.
- ◆ Consult with local authorities about restricting access to the buffer zone around the facility. Evaluate the need for closing or restricting traffic on nearby roads, waterways, or public access areas adjacent to the facility. Implement measures as determined to be appropriate.
- ◆ Redirect mail, shipments, and deliveries to areas distant from sensitive or critical assets. Accept deliveries only during daytime hours.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.
- ◆ Ensure all High Alert (HSAS ORANGE) measures listed above are implemented.
- ◆ Close the facility and cancel events, where applicable, until the threat has been reduced.
- ◆ If the decision is made to keep the facility open and proceed with an event, where applicable: reduce access to an absolute minimum and consistent with patron emergency egress needs and fire codes, where applicable; allow no access to non-employees; halt all contractor work; allow no visitors; do not accept any nonessential mail, shipments, or deliveries.



BARRIERS

Considerations

Baseline Countermeasures (HSAS **YELLOW**)

- ◆ Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the building. Evaluate natural features (e.g., hills, woods, waterways) that could either enhance or inhibit security at the facility. Consider delay time created by barriers and evaluate for adequacy.
- ◆ Install appropriate perimeter barriers and gates. Implement an appropriate level of barrier security (e.g., chain-link fences, chained gates, remotely closed gates). Maintain a clear area at perimeter barriers to enable continuous monitoring and to inhibit concealment of people or packages. Inspect the perimeter barrier regularly.
- ◆ Install alarms and intrusion detection equipment at perimeter barriers.
- ◆ If appropriate, install interior building barriers (e.g., internal locked doors) to protect sensitive or critical areas or corridors within a building.
- ◆ Ensure that the facility has smoke-proof stairways and exit corridors that can be used for evacuation.
- ◆ Install barriers at HVAC systems (e.g., screens on intakes, filters) to prevent the introduction of chemical, biological, or radiological agents into the building. Where needed, provide positive pressure in building to prevent contaminants from entering. Train staff in emergency shut-off procedures for HVAC systems.
- ◆ Ensure that HVAC intakes are covered by screens so that objects cannot be tossed into the intakes or into air wells from the ground.
- ◆ Move objects that could become projectiles (e.g., trash containers, crates, loose items not attached to a building or to the ground) a safe distance from buildings and areas where large numbers of people congregate.
- ◆ Install barriers to protect doors and windows from the effects of small arms firing and explosive blasts (e.g., blast-resistant and shatter-resistant glass, offset entryways, shrubbery).
- ◆ Ensure that exterior doors have hinge pins that cannot be removed from the outside and that there are no gaps between the door and jamb that would allow for the door to be compromised.
- ◆ Where needed, provide positive pressure in building to prevent contaminants from entering. Train staff in emergency shut-off procedures for HVAC systems.



- ◆ If appropriate, erect temporary jersey barriers at or around structures where they are not already in place.
- ◆ Use vehicles as temporary physical barriers by placing them in front of buildings/structures or across roads.
- ◆ Where appropriate, position gates and perimeter boundary fences outside the blast vulnerability envelope, when possible.
- ◆ Review landscaping and ensure that buildings are not obscured by overgrowth of bushes or shrubs where contraband could be placed or adversaries could hide.
- ◆ Evaluate vehicle and vessel traffic patterns around the dam and vital facilities. Design and implement traffic control strategies and barriers (e.g., road alignment, serpentine traffic routing, retractable bollards, swing gates, speed bumps, tire shredders) to control vehicle speed and approaches to sensitive or critical assets.
- ◆ Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from the building and areas where large numbers of people congregate to provide increased stand-off distance.
- ◆ Install bollards on pedestrian walkways to keep vehicles off them.

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Install all barriers and repair as needed.
- ◆ Deploy additional temporary barriers (e.g., Jersey barriers, heavy vehicles and equipment, log booms, barges, empty containers) to increase the stand-off distances from the facility, and between vehicles and buildings.
- ◆ Deploy additional temporary barriers to slow and control the direction of traffic into the facility and within the facility.
- ◆ Relocate critical items (e.g., specialized equipment, important records) to areas of the facility with higher levels of physical security.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.
- ◆ Ensure all High Alert (HSAS Orange) measures listed above are implemented.
- ◆ Increase the number and security of barriers to the maximum extent possible consistent with the operating level of the facility.





COMMUNICATION AND NOTIFICATION

Considerations

Baseline Countermeasures (HSAS YELLOW)

- ◆ Develop a communication and notification plan that covers voice, data, and video transfer of information related to security.
- ◆ Install system(s) that provide communication with all people at the facility, including employees, contractors, security force, emergency response teams, visitors and patrons, guests, and tenants.
- ◆ Provide redundant communication channels (e.g., telephone, radio, pager, public address system) that can be used in the event one channel is disabled. Provide backup electric power (e.g., backup generators, uninterruptible power supplies) to run communications equipment.
- ◆ Install a special “panic alarm” systems in sensitive or critical areas.
- ◆ Installation a priority access communication system to give preferred access to users involved in emergency management.
- ◆ Test systems regularly.
- ◆ Train employees in the use of the various communications systems.
- ◆ Install system(s) that provide communication channels with local law enforcement and emergency responders. Provide redundant communication channels and backup power. Test systems regularly.
- ◆ Have emergency communication equipment (e.g., special cell phones, emergency radios) available for use in the event all primary communication channels are unavailable.
- ◆ Provide communication security (e.g., encryption, multiple frequencies) that will prevent unauthorized interception of information being transferred. Regularly conduct countermeasure sweeps of the communications systems to uncover any eavesdropping or other security compromises. Train employees not to discuss sensitive information over communications channels that are not secure (e.g., cell phones). Provide the ability to record incoming communications (e.g., telephone calls) to identify potential threats.
- ◆ Confirm that communication systems are interoperable between facility organizations and with 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 restoring service if a disruption occurs.



- ◆ Develop a notification protocol that outlines who should be contacted in emergencies. Maintain and provide a contact list to all who might need it. Keep the list up to date. Regularly test notification protocol through drills and exercises.
- ◆ Provide a simple and straightforward means for people to communicate the presence of a potential threat or an emergency (e.g., a hot line number, internal 9-1-1 capability).
- ◆ Develop a process for communicating to facility management employees and tenants 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.
- ◆ Establish call-in procedures for employees who work in remote or isolated locations. Utilize these procedures for both routine and emergency situations.
- ◆ Ensure that the security force can communicate easily in all languages that a significant portion of the customer, patrons, or tenants speak.
- ◆ Develop a process for communicating with the public and the media regarding security. Identify the people who will be responsible for media interactions. Provide adequate information to quell rumors and dispel unnecessary alarm. Take steps to restrict the release of information that might compromise the facility's security.
- ◆ Monitor industry and government information on threats, incidents, and response procedures. As appropriate, share information on the building's experiences.

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Increase the frequency of communications with local law enforcement. Advise them of increased security status of the facility. Identify additional security measures that will be implemented.
- ◆ Increase communication with employees about the security situation and provide reminders of actions to take in the event of an incident (i.e., evacuation, sheltering in place).
- ◆ Increase frequency of reporting and call-ins from employees, particularly those working in remote areas and areas isolated from the facility.
- ◆ Test communications equipment, including primary and backup systems, more frequently.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.



- ◆ Ensure all High Alert (HSAS ORANGE) measures listed above are implemented.
- ◆ Maintain communication with local law enforcement as continuously as is sustainable.
- ◆ Provide employees with as much information as possible as frequently as possible to keep them apprised of the security situation. Update personnel on any escalating threat.
- ◆ Have communication backup equipment activated and ready for possible use.



MONITORING, SURVEILLANCE, INSPECTION

Considerations

Baseline Countermeasures (HSAS **YELLOW**)

- ◆ Evaluate needs and design a monitoring and counter surveillance program that is consistent with facility operations and security requirements. Coordinate with local law enforcement on activities to be undertaken, particularly with regard to monitoring activities in the surrounding area outside the facility.
- ◆ Provide visual surveillance capability (e.g., designated surveillance points, cleared lines of sight) for sensitive and critical assets at the facility. Assign and train personnel, including security force and other employees, to maintain vigilance to unusual activities in sensitive or critical areas. Keep surveillance areas clear of obstructions (e.g., vegetation, parked vehicles) that would inhibit observation.
- ◆ Install video surveillance equipment (e.g., closed-circuit television [CCTV], lighting, night vision equipment). Provide coverage for the perimeter, sensitive and critical assets, vehicle roadways and parking lots, and entrances. Include coverage of buffer zone around the facility. 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/or to other organizations outside the facility. Inspect and test all video equipment regularly.
- ◆ Install detector and alarm systems. Include intrusion detectors, fire and smoke alarms, motion detectors, CBR material detectors, and explosives detectors as appropriate. 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. Review recordings regularly for unusual activities or patterns. Establish procedures to secure detector and alarm recordings for forensic purposes. If appropriate, provide detector and alarm feed to local law enforcement and/or to other organizations outside the facility. Inspect and test all equipment regularly.
- ◆ Develop procedures to use trained and certified dogs to check for explosives or other dangerous items.
- ◆ Mount digital security cameras on high structures such as roller coasters at an amusement park. These can be used to assist security on the ground in finding a customer who is trying to avoid security.
- ◆ If appropriate install GPS equipment on facility vehicles to monitor their location. Train employees monitoring the GPS feeds to recognize potential security-related events. Establish procedures for responding to these events.
- ◆ If appropriate, ensure that the facility (e.g., stadium, arena) has an intrusion detection system (IDS) that is connected to a local security company and/or local law enforcement.



- ◆ If appropriate, provide adequate lighting to illuminate the entire facility (e.g., stadium, arena); integrate the lighting system with backup power in the event of an emergency. Ensure that lighting fixtures and remote cameras have vandalism-proof covers or are located high enough to prevent damage caused by vandalism.
- ◆ If appropriate, provide video surveillance systems on facility (e.g., stadiums, arenas) grounds, in parking lots, and in buildings. Ensure that remote camera locations provide maximum coverage of the grounds. Make sure that the view angles of security cameras are free and unobstructed by buildings, trees, or other structures.
- ◆ Assess the adequacy of closed-circuit television (CCTV) coverage and install additional CCTV cameras in areas where they are needed.
- ◆ Install a conventional explosives detection system.
- ◆ Install personnel/car/baggage screening detection capabilities, such as scanners, if they are not already in place.
- ◆ Deploy the security force to regularly inspect facility perimeter, buildings, parking lots, locker rooms, equipment, trash containers, HVAC systems, and sensitive or critical areas for signs of security issues. Ensure that the security force has access to all areas to be inspected. Implement both random and scheduled inspections. Utilize plain-clothes and uniformed patrols. Utilize vehicle, foot, and bicycle patrols as appropriate. Pay special attention to assets that are not used frequently. Train security force and other employees on items they must be alert to and on reporting procedures.
- ◆ Continuously monitor people entering and leaving the building. Train monitors to detect suspicious behavior (e.g., unusually bulky clothing that might conceal weapons, unusual packages being carried).
- ◆ Monitor work being done adjacent to the facility (e.g., road construction, utility equipment servicing) for signs of unusual activities (e.g., someone photographing the facility).
- ◆ Inspect delivery vehicles entering the facility.
- ◆ Inspect packages, briefcases, backpacks, parcels, and luggage being carried by people, including employees, contractors, vendors, and visitors. Perform either a spot check or comprehensive inspection. Include hand searches of packages, metal detectors, X-ray scanners, or explosive-sniffing dogs. Provide more thorough inspection for those entering sensitive or critical areas. Inspect persons who are leaving as well as entering.
- ◆ Monitor the activities of contractors, delivery personnel, and vendors while they are at the facility for unusual behavior.
- ◆ Continuously monitor all vehicles and vessels approaching the facility for signs of threatening behavior (e.g., driving at an unusually high speed, approaching restricted areas). Be prepared to take defensive action against vehicles or vessels exhibiting such behavior (e.g., engage barriers, deploy security force vehicles or boats).



- ◆ Inspect all deliveries. 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. 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., bills of lading, invoices).
 - ◆ Inspect all mail for unusual characteristics (e.g., strange powders, leaking material, no return address). Divert such mail to a controlled area for handling. Provide personal protective equipment for those handling suspicious mail or packages.
 - ◆ Advise employees to check all deliveries and mail at home for suspicious material.
 - ◆ Regularly inspect all supplies for signs of tampering.
 - ◆ Acquire luggage-screening equipment for use during high-threat and/or high-profile events.
 - ◆ Implement quality control inspections on food supply if appropriate (e.g., hotels, special events). Conduct background investigations on food suppliers.
 - ◆ Pick up and secure all loose items, such as trashcans, benches, newspaper racks, cigarette urns, traffic cones, barriers, free-standing signs, recyclable containers, or any items not attached to a permanent structure.
 - ◆ Maintain a thorough inventory and accounting of all sensitive or critical materials and equipment and their storage and movement into, out of, and within the facility.
 - ◆ Monitor contractor work performed at the facility (e.g., construction, equipment installation, maintenance, cleaning) for signs of unusual activities. Inspect all work before releasing the contractor.
 - ◆ Monitor work being performed adjacent to the building (e.g., road construction, utility equipment servicing) for signs of unusual activities (e.g., photographing of the facility, planting of packages near facility perimeter or assets).
- Protective Measures during Periods of High Alert (HSAS ORANGE)**
- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
 - ◆ 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.
 - ◆ Increase monitoring of video surveillance, alarms, and detector equipment feeds. Route suspicious detector feeds to local law enforcement.



- ◆ Install additional temporary lighting to illuminate all areas. Leave lighting on 24 hours. If possible, increase lighting in the buffer zone.
- ◆ Restrict items that people are permitted to carry into the facility.
- ◆ Deploy portable scanning equipment (e.g., metal detectors, X-ray scanners) to increase the level of inspection.
- ◆ Isolate or remove any HAZMAT that might increase the impacts of an attack.
- ◆ Increase frequency and thoroughness of inspections of buildings and facility assets to the maximum level sustainable. Close and secure nonessential buildings and assets.
- ◆ Search all persons entering the facility. Restrict the number of people allowed to enter to essential personnel only.
- ◆ Restrict the vehicles permitted to approach the facility to essential needs only.
- ◆ Thoroughly inspect all mail and deliveries made to the facility. Postpone all nonessential deliveries. Process mail and deliveries at remote site.
- ◆ Deploy portable scanning equipment (e.g., metal detectors, X-ray scanners) to increase the level of inspection.
- ◆ Check all security systems, such as lighting and intruder alarms, to ensure they are functioning.
- ◆ Increase tracking of certain HAZMAT and munitions movements.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.
- ◆ Ensure all High Alert (HSAS Orange) measures listed above are implemented.
- ◆ Increase staff assigned to surveillance, monitoring, and inspection duties to a maximum sustainable level. Request additional support from local law enforcement.
- ◆ Increase the frequency and thoroughness of monitoring and countersurveillance activities to the maximum level sustainable. Request additional support from local law enforcement agencies.
- ◆ Increase frequency and thoroughness of inspections of buildings and facility assets to the maximum level sustainable. Close and secure nonessential buildings and assets.
- ◆ Thoroughly inspect all mail and deliveries made to the facility. Postpone all nonessential deliveries. Process mail and



deliveries at a remote site.

- ◆ Implement continuous monitoring of video surveillance, alarms, and intrusion detection feeds.
- ◆ Search all persons entering the facility. Prohibit packages from being brought into the facility. Restrict the number of people allowed to enter to essential personnel only.
- ◆ Inspect all vehicles and their contents before allowing them to enter the facility. Restrict the number of vehicles permitted to enter to essential needs only.
- ◆ Pick up and store all loose items, such as trashcans, benches, newspaper racks, cigarette urns, traffic cones, barriers, free-standing signs, and recyclable containers or any items not permanently attached to a structure.
- ◆ Conduct frequent checks of building exteriors and parking areas.



CYBER SECURITY

Considerations

Baseline Countermeasures (HSAS YELLOW)

- ◆ Develop and implement a security plan for computer and information system hardware and software. Design and implement secure computer network architecture.
- ◆ Develop a recovery and restoration plan to return computer systems to full functionality after an incident. Determine the ability to manually relocate essential computer equipment in the event of an incident. Identify sources for replacement equipment that could be brought into service quickly.
- ◆ Regularly back up critical data and store off-site.
- ◆ Regularly test the computer security measures (e.g., audits, penetration testing).
- ◆ 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 address cyber security issues. Conduct periodic background checks on employees serving as system administrators.
- ◆ Carefully validate the credentials of all contractors and vendors given access to computer systems. Monitor and review their work when completed.
- ◆ Provide training on cyber security threats to all employees who use facility computer systems. Consider e-mail phishing; deceptive inquiries from outsiders; malicious code, such as viruses, worms, and Trojan horses. Look into measures for protecting the system and train employees about their cyber security responsibilities, such as changing passwords regularly, refraining from divulging computer information to others, and not opening unknown e-mail attachments. Immediately cancel computer access for terminated employees.
- ◆ Install and maintain up-to-date cyber security 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. Stay up to date on the latest cyber security threats, incidents, and defensive measures.
- ◆ Control physical access to IT facilities (e.g., computer rooms, automated control systems). Install locks and access controls to allow only authorized personnel to enter. Provide communication capabilities to allow rapid reporting of incidents.
- ◆ Control both on-site and off-site 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 and vital equipment in the event that primary systems are disabled. Back up computer files regularly. Maintain back-up media in a separate and secure location.
- ◆ Thoroughly test all applications that involve handling of sensitive information or which control vital electro-mechanical systems to determine their potential vulnerability to compromise.
- ◆ Regularly review facility Web site to ensure no sensitive information is provided.

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Delay scheduled maintenance and upgrades on software and hardware that is not security related; increase frequency of system backups. Ensure that backups are taken off-site for storage.
- ◆ Increase monitoring of system probes, intrusions, and other anomalies.
- ◆ Reduce number of people authorized to access computer systems.
- ◆ Ask employees to increase their vigilance with regard to unusual activities.
- ◆ Reduce access to the Internet; restrict instant messaging and peer-to-peer applications.
- ◆ Commit time for technical support personnel to address any problems.
- ◆ Delete any information from the facility Web site that might aid an adversary in planning an attack.
- ◆ Establish communications with utility service providers to review plans for responding to any disruptions.
- ◆ Where possible, provide additional backup utility supplies (e.g., backup generators).

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (HSAS ORANGE) measures listed above.
- ◆ Ensure all High Alert (HSAS Orange) measures listed above are implemented.
- ◆ Increase computer security to maximum levels.



- ◆ Reduce access to the Internet and other portals to the absolute minimum.
- ◆ Have technical support available on-call 24/7.
- ◆ Provide continuous monitoring of computer system for anomalies.
- ◆ Restrict computer access to essential personnel only.
- ◆ Disable the facility's Web site.



INFRASTRUCTURE INTERDEPENDENCIES

Considerations

Baseline Countermeasures (HSAS **YELLOW**)

- ◆ Ensure that the facility has adequate utility service capacity to meet normal and emergency needs. Identify all utility service points that support the facility. Establish regular communication channels with utility service providers (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.
- ◆ To the extent possible, 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.
- ◆ Provide adequate physical security (e.g., fencing, locks, protective enclosures, access restrictions) for utility services, fuel storage containers, trash dumpsters, and HVAC systems. Include installation of special locking devices on utility access points (e.g., manhole covers, HVAC vents).
- ◆ Maintain regular communication channels with utility service providers to understand (a) actions to be taken in response to a loss of service from primary supply sources, (b) restoration priorities, and (c) alternatives.
- ◆ Ensure that key employees and security personnel are familiar with procedures for shutting off utility services (e.g., electricity, natural gas, HVAC systems) in emergency situations.
- ◆ Locate dumpsters and other large trash containers away from facility structures to provide greater standoff distance.
- ◆ Monitor dumpsters and trash containers to prevent (a) hiding of explosives or other hazardous materials and (b) unauthorized access to discarded papers and records.
- ◆ Where practical, provide for redundancy and emergency backup capability for critical utility services (e.g., backup electric power generators, multiple utility feeder lines). Where possible, locate the redundant and backup equipment in a different part of the facility from the primary supply equipment. Inspect and maintain redundant and backup equipment regularly.
- ◆ Understand the transportation methods used by employees (e.g., private vehicle, subway, bus, transit rail) to get to and from work and the effects of a transportation disruption on facility operations. Develop alternatives.
- ◆ Provide for regular monitoring and inspection of utility services (e.g., security force patrols, CCTV) and their security measures. If applicable, provide 24/7 guard at utility supply points starting 24 hours before a special event until its conclusion.
- ◆ Develop plans for decontamination (e.g., from chemical, biological, radiological agents) of infrastructure facilities.



- ◆ Connect ductwork smoke detectors into the fire alarm system and design the system to automatically shut down the air-handling units.
- ◆ Secure dumpsters and other trash containers to prevent the hiding of explosives or other hazardous materials and to prevent unauthorized access to discarded papers and records. Make sure the gate side is lockable and provides visual access to the inside of the enclosure.
- ◆ Provide appropriate IT and telecommunications security controls and technologies to (a) control access to facility data and automated processes and (b) prevent viruses, hackers, and insider exploits.
- ◆ Develop communication protocols with downstream companies (i.e., those to whom you supply goods or services) to inform them of product delivery issues.
- ◆ Evaluate alternative vendors for facility trash removal and provision of cleaning staff in case primary vendor service is disrupted. Work with vendors to vet their personnel and develop a process to provide access badges and identification to new cleaning crews.
- ◆ Evaluate how money is brought in, stored, distributed, and used and how excess funds are transported between the facility and banks.
- ◆ Evaluate the security of online sales systems (Web sites) and provide adequate privacy protections for transactions and customer data.
- ◆ Evaluate dependence on emergency services agencies to provide additional staff for sporting and entertainment events.
- ◆ Evaluate multi-jurisdictional environments, i.e., those in which a facility spans different emergency services jurisdictions (local, State, national), and establish working relationships with all parties. Develop and exercise response plans to ensure that each jurisdiction understands its role.
- ◆ Understand and evaluate the risk of nearby hazards to your facility (e.g., underground pipelines, hazardous chemical sites, airports, nearby freight rail lines, rail lines that pass under the facility, nearby waterways, earthquake faults).

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Increases monitoring, inspection, testing, and patrols of all utility services. Request assistance from local law enforcement.
- ◆ Review and implement actions specific in the emergency response plans. Adjust as necessary to deal with specific incident conditions.



- ◆ Activate facility emergency operations center as appropriate.
- ◆ Add emergency response personnel (e.g., firefighters, emergency medical staff) to shifts.
- ◆ Pre-position emergency response personnel and equipment to locations that would enable rapid response to an incident.
- ◆ Evaluate alert situation and impact on operations to facility inputs and outputs. Initiate changes as needed. Notify affected employees.
- ◆ Notify suppliers of alert situation and any facility operation changes. Notify suppliers of any changes in security that they should be aware of to make deliveries (e.g., advance notification of arrival, different entry gate, vehicle inspection points, driver credentials, special identification code words).
- ◆ Establish communication with utility service providers (e.g., water, wastewater, electricity, natural gas) and review response plans to handle service disruptions.
- ◆ Perform a special backup of IT data and transporting the back-up media offsite when completed.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (**HSAS ORANGE**) measures listed above.
- ◆ Provide continuous monitoring of all utility services. Provide a continuous security guard presence at critical utility points.
- ◆ Review available threat information and determine whether the stadium or arena should be closed and events canceled. Evaluate criteria regarding when the stadium or arena should be reopened or restored to full operation.
- ◆ Bring emergency operations center up to full capability on a 24/7 basis.
- ◆ Inspect all transportation shipments prior to entry into the facility.
- ◆ Notify suppliers and customers of the impacts of the alert on your facility and inform them whether the facility plans to continue operations.
- ◆ Evaluate the need for continued operation of Web sites and customer portals that allow front-end facility processes. Shut down if not needed.
- ◆ Back up IT data and move the back-up media to a protected facility off-site.
- ◆ Establish and maintain communications with emergency services facilities that support the facility. Test redundant



communications systems.



INCIDENT RESPONSE

Considerations

Baseline Countermeasures (HSAS **YELLOW**)

- ◆ Develop and maintain an up-to-date emergency action plan (EAP) (see Planning and Preparedness).
- ◆ Develop a plan to ensure all patrons, employees, etc., are evacuated from the facility for such incidents as bomb threats. If possible, employ security guards knowledgeable in foreign languages that patrons, customers, tenants, employees, etc., might speak.
- ◆ Maintain a list of specialized responders, with phone numbers and other contact information. Include persons who speak foreign languages, helicopter rescue operators, crane and high-reach equipment companies, and other emergency responders.
- ◆ Ensure that an adequate number of facility management emergency response personnel are on duty and/or on call at all times. Ensure that back-up personnel can execute emergency response functions in the event that primary personnel are unavailable or incapacitated. Ensure that adequate equipment and supplies are available to support emergency response requirements.
- ◆ Review unified incident command procedure for responding to an event with local law enforcement, emergency responders, and government agencies and test/exercise the procedures.
- ◆ Prepare an emergency operations center or emergency command center that can be used to coordinate resources during an incident. If necessary, consider a backup center for use in the event the primary center is disabled. Consider the use of mobile command centers.
- ◆ Provide training and equipment to facility management emergency response personnel to enable them to deal with terrorist-related incidents (e.g., CBR agents, suicide bombers). Conduct regular drills and tabletop exercises with emergency response teams. Involve local emergency responders in drills and exercises.
- ◆ Encourage employees to participate in community and other outside organization emergency preparedness and response training.
- ◆ Check the status of all emergency response equipment and supplies on a regular basis and more frequently prior to an event. Locate emergency supply kits in areas where employees can have ready access to them. Provide adequate security for emergency response equipment, facilities, and personnel. Do not leave emergency vehicles or equipment unattended or unsecured.



- ◆ Identify entry and exit points to be used in emergencies. Ensure that they are free of obstructions and can be fully utilized. Inspect regularly for signs of tampering and intentional obstruction. Train all employees on the location of these points.
- ◆ Identify alternate rallying points where employees and others at the facility can gather for coordinated evacuation and/or for “head counts” to ensure that all have been evacuated. Identify alternate transportation routes for employees and others at the building for use during evacuations. Test the routes with drills and exercises.
- ◆ Maintain an inventory of long-lead-time equipment and supplies that can be readily available for deployment after an incident.
- ◆ Develop a list of key personnel who can be pre-credentialed to gain access to the building after an incident and assist with recovery activities.
- ◆ Develop policies and procedures for dealing with the media and the public in the event of an incident to advise them of the situation and to defuse rumors and panic.
- ◆ Establish procedures for facility evacuation and for shelter-in-place situations. Check accommodations for evacuating physically, mentally, visually, and hearing-impaired persons. Review the organized search procedure to ensure all guests and employees are evacuated. For evacuations, ensure that the hotel has smoke-proof, pressurized exit stairways. For shelter-in-place situations, ensure that an adequate facility is available and sufficiently stocked with food, water, and supplies to accommodate the number of people who might need to use it.
- ◆ Develop plans to assist the families of facility emergency response teams in the event the teams must be away from home for extended periods.
- ◆ Develop plans to provide counseling to employees in the aftermath of an incident.
- ◆ Implement procedure for capturing lessons learned and developing revised response plans after an incident.

Protective Measures during Periods of High Alert (HSAS ORANGE)

- ◆ Ensure you have implemented all Baseline Countermeasures (HSAS YELLOW) listed above.
- ◆ Review and implement emergency response plans. Adjust as necessary for conditions.
- ◆ Activate facility emergency operations center as appropriate; notify law enforcement personnel.
- ◆ Add emergency response personnel to shifts.
- ◆ Delay vacation or travel for critical facility personnel. Ensure that all personnel responsible for implementing countermeasures are immediately available.



- ◆ Pre-position emergency response, including engineering response, personnel and equipment to enable rapid response.
- ◆ Review, revise, and implement contingency plans that may be needed (e.g., review procedures with employees assigned to direct facility traffic, direct crowd control, guide first responders [if needed], or shut off utilities during an incident).
- ◆ Prepare to execute contingency plans, such as moving personnel to an alternate location. Release all noncritical facility personnel.
- ◆ Review procedures with employees assigned to shut off utilities (e.g., electricity, water, gas) in the event of an incident.
- ◆ Exercise increased vigilance regarding the use of electronic banking and credit transactions.
- ◆ Keep all personnel responsible for implementing antiterrorist plans on call and readily available.

Protective Measures during Periods of Severe Alert (HSAS RED)

- ◆ Ensure you have implemented all High Alert (**HSAS ORANGE**) measures listed above.
- ◆ Ensure that all High Alert (HSAS ORANGE) measures listed above are implemented.
- ◆ Review available threat information and determine whether the facility should be closed or should operate with reduced hours and/or a reduced work force and/or reduced activities. Evaluate whether events should be cancelled. Evaluate criteria for when facility should be reopened or restored to full operation.
- ◆ Bring emergency operations center up to full capability on a 24/7 basis. Assign emergency response personnel.
- ◆ Cancel all vacation and travel for facility personnel.
- ◆ Advise the public to develop back-up plans to address their financial needs in the event of closure of access to electronic banking and credit transactions. Review with emergency operations center staff the emergency response plans and protective action guides for potential radiological emergencies.
- ◆ Ensure the availability of critical provisions (i.e., food, water) for the emergency operations center staff and security/guard personnel who may be working extended hours.
- ◆ Check all available emergency equipment.
- ◆ Pre-position and mobilize specially trained teams or special resources.
- ◆ Add firefighter and emergency medical personnel to shifts.
- ◆ Implement emergency and continuity plans as appropriate.



- ◆ Increase or redirect personnel to address critical emergency needs.
- ◆ Assign emergency response personnel and pre-position and mobilize specially trained teams or resources.



UNIQUE MEASURES

Considerations

Public Assembly. Areas for public assembly facilities to focus implementation of protective measures include the following:

- ◆ Access controls: (a) control over who obtains tickets to an event and inspections of items individuals bring into a facility, (b) background checks for set-up and maintenance crews, (c) inspections on equipment and materials brought into a facility by crews, (d) accessibility of peripheral areas such as a queue for ticket purchase outside of an access control point, or open free parking lots with no attendants, (e) security controls for vehicles entering an attached or peripheral parking area.
- ◆ Building systems: As with all enclosed buildings and depending on specific system designs, convention centers are vulnerable to explosives; arson; chemical; biological, or radiological contaminants introduced into HVAC systems; blocked emergency exits; and similar building vulnerabilities.
- ◆ Concession food contamination: Food supplied to concessionaires is often not inspected and may not be secured.
- ◆ Publicly-announced details of scheduled events.
- ◆ Ticket sales managed by independent ticket-selling organizations: Need for protective measures against a cyber attack on the ticket-selling process that could seriously impact the performance organizations.

Sports Leagues. Areas for sports leagues to focus implementation of protective measures include the following:

- ◆ Event-day access controls: Access control to the facility is an important protective measure utilized during sporting events. It is important to control vehicles and individuals outside the facility, inside the facility, and in restricted or playing/racing areas. Access control is implemented in terms of three perimeters (i.e., outer, middle, and inner).
- ◆ Outer access controls: A secure outer perimeter (i.e., buffer zone) of at least 100 feet should be established around the facility to the maximum extent and when possible. This outer perimeter is used to deter vehicle traffic, but not necessarily pedestrian traffic. It often encompasses the facility's property boundary, but this differs for each facility. The outer perimeter may include the facility's parking lots and, in the case of motor speedway events, the camping areas.
- ◆ Middle access controls: The middle perimeter is the first level of access control for persons and their possessions. This perimeter is secured so that no one without a pass/ticket or credential is permitted entry through protected gates or doors. At motor sport facilities, the middle perimeter usually encompasses the outer ring of the racing surface and the stands. Unlike other major sporting events, it is also the first line of defense for vehicle access.
- ◆ Inner access controls: For sport team events, the inner perimeter contains the players' locker rooms, benches, playing



surface/racetrack, infield, and garage/pits. For motor sport facilities, the inner perimeter includes the track surface and the infield. The size of this perimeter varies from track to track, potentially including camp grounds, helipads, vendors, fuel stations, garage areas, and pits. At motor sport venues, the inner perimeter contains all high-level government officials, competitors, sponsors, entertainers, and event officials. No one should be permitted in the inner perimeter without proper credentials and identification.

- ◆ Event-day signage: Signage is essential to the orderly conduct of an event, and proper signage should include the following: Point of Contact information for facility security personnel with guidance for responding to and reporting suspicious activities; lists of prohibited items; clear identification of exit points and emergency exits; identification of the type of access allowed in a particular area.
- ◆ Even- day gate access and management, including: train, equip, and supervise employees in proper inspection procedures and identification of suspicious items; post uniformed police officers at each gate to observe suspicious behavior; create policy to identify an item forbidden within the facility, and publicize the list of prohibited items and the inspection policy; designate an entrance for all concessionaires, gatekeepers, ushers, and cleaning personnel.
- ◆ Event-day personal searches: Personal searches may include visual inspections, pat-downs, metal detectors, and/or inspection of items brought into the stadium. Facility management as well as individual sports teams should take into consideration the type of sporting event, the teams/event participating, past event history, team requests, and current world climate when making decisions regarding personal and visual searches.
- ◆ Event-day credential procedures: Credential systems should indicate (a) areas of access/event function; (b) areas of sensitivity (protective measure needs, facility needs, event needs, media needs, and financial control needs); and, purpose of activity on facility premises.
- ◆ Ensure that all food concessions are reasonably secure, inspect food packages and containers for tampering, and implement policy for identifying and reporting suspected food tampering.
- ◆ Event-day aviation: Involve the FAA when planning and conducting any on-site events that include aviation activities. The FAA is required to issue a Special Notice pursuant to 14 CFR 99.7.
- ◆ Event-day security for teams and officials: If an incident requires immediate evacuation, both the visiting and home teams, as well as event officials should be escorted to a pre-determined, secure location by facility security personnel. The designated location should be communicated by the facility to the League Security Office at the beginning of each season.

Resorts. Areas for resorts, and in particular casinos, to focus implementation of protective measures include the following:

- ◆ Measures to mitigate the vulnerability posed by having large amounts of cash on hand. Casinos have extensive security measures to deal with this risk.



- ◆ Unrestricted public access to casinos. Depending on the type of structure and the security measures in place, casinos may or may not be able to control access to the facility by potential adversaries. Many people carry luggage, backpacks, and other packages that have not been inspected through casinos.
- ◆ Access to peripheral areas. People often congregate outside a casino, and vehicles entering contiguous parking lots and/or drop-off areas are generally not inspected for weapons or explosives.
- ◆ Access to casinos by workers, suppliers, and maintenance staff that may not have undergone background checks. Background checks should at least include criminal history. In addition, inspections of the equipment and materials brought in by these crews should be performed.
- ◆ Measures to manage evacuation of congested gaming areas, as well as mitigate the impact of alcohol consumption on the ability of patrons to evacuate effectively.
- ◆ Secure building systems (i.e., heating and cooling, emergency exits) to decrease vulnerability to explosives, arson, and CBR contaminants.
- ◆ Focus the training of personnel and the orientation of security equipment (i.e., video surveillance) to include detection of terrorist events as well as conventional theft and cheating incidents.
- ◆ Closely monitor the on-site storage on chlorine to purify water in swimming pools or for drinking water to avoid accidental release of the chemical.

Lodging. Areas for lodging facilities to focus implementation of protective measures include:

- ◆ Unrestricted public access, unrestricted access to peripheral areas, and unrestricted access to areas adjacent to buildings.
- ◆ Access by suppliers, vendors, and maintenance workers to nonpublic areas.
- ◆ Employee background checks and increase training and equipping of security force.
- ◆ Emergency operations plans and exercises for emergency plans.
- ◆ Protection of HVAC systems and other utility services (i.e., electric, power, natural gas, telecommunications, water supply) that are not secured or monitored for intrusion.
- ◆ Building design to incorporate characteristics like shatter or blast-resistant glass, structural supports that can handle large overpressures from explosives, and tamper-resistant doors and windows.
- ◆ Monitoring of locations (i.e., trash containers, planters, counters, and decorative fixtures) where explosives or hazardous agents could be placed.



Outdoor Events. Areas for outdoor events to focus implementation of protective measures include:

- ◆ Access controls: Many large outdoor public gatherings do not have access controls. Some major events have gated areas where participants may be screened, but these events are limited to a few high-profile gatherings. Many events have a significant security presence, but the ability to monitor the crowd, including what items they may be carrying to the event, is limited. Additionally, access controls should be considered for vehicles entering parking lots or areas around large outdoor public gatherings.
- ◆ Temporary structures: Because of their transitory nature, many events require easily constructed temporary structures. These temporary structures are often neither designed nor erected to withstand stresses other than those from intended use. These structural deficiencies may be exploited by adversarial elements, and monitoring of construction crews and of any dangerous materials they may place in the structures may be limited.
- ◆ Event/activity atmosphere: The frequent congestion, noise, and disorganization of and outdoor public gathering provide opportunity for an adversary to hide a package containing dangerous materials, discharge a weapon or explosive, or carry out other methods of attack. Incidents in large crowds can easily lead to chaos and panic. Crowd control and evacuation plans must be prepared and exercised.

Entertainment and Media. Areas for entertainment and media facilities to focus implementation of protective measures include:

- ◆ Development and testing of emergency plans.
- ◆ Public/private sector emergency response coordination.
- ◆ Training.

Real Estate. Areas for the Real Estate Subsector to focus implementation of protective measures include:

- ◆ Perimeter and site security.
- ◆ Building designs that incorporate security considerations.
- ◆ Control of vehicular traffic around and into a building.
- ◆ Security in parking areas, loading docks, shipping and receiving areas, and mailrooms.
- ◆ Access controls to channel access through entry control points where identity verification devices can be used for screening.
- ◆ Security on HVAC systems and other building utilities (e.g., electric, natural gas/propane/fuel, water, sewer, flooding,



communications, storage tanks).

- ◆ Security policies and emergency plans that are enforced and exercised.
- ◆ Fire protection capabilities.
- ◆ Ensure that information on building design and construction are secured and access-controlled, and not publicly available.

Retail. Areas for the Retail Subsector to focus implementation of protective measures include:

- ◆ Access controls: Openness to the public is a key vulnerability of shopping centers. Security personnel should be utilized to monitor patrons and any suspicious activity. Additionally, there is very little or no control of the large number access points to a shopping mall. Malls can use CCTV to maintain surveillance of access points. Parking lots and/or garages should be monitored for vehicles that could present a threat. Unrestricted vehicle access to areas adjacent to buildings (i.e., patron drop-off/pick-up points) also presents at threat in that vehicles stopped at these points are generally not inspected for weapons or explosives. Finally, suppliers, vendors, and maintenance workers with access to nonpublic areas should be screened and their vehicles searched before accessing loading docks, mailrooms, or service entrances that are not secured or monitored.
- ◆ Employee background checks of facility personnel.
- ◆ Security force: Many retail facilities do not employ their own security force, and rely on local law enforcement to handle incidents. Facilities that do employ a security force may use various methods to train and equip security guards. Coordination between facility security force and local law enforcement is essential.
- ◆ Exercises of emergency plans.
- ◆ Protection of HVAC systems and other utility services (e.g., electric power, natural gas, telecommunications, water supply). These systems should be secured and monitored for intrusion.