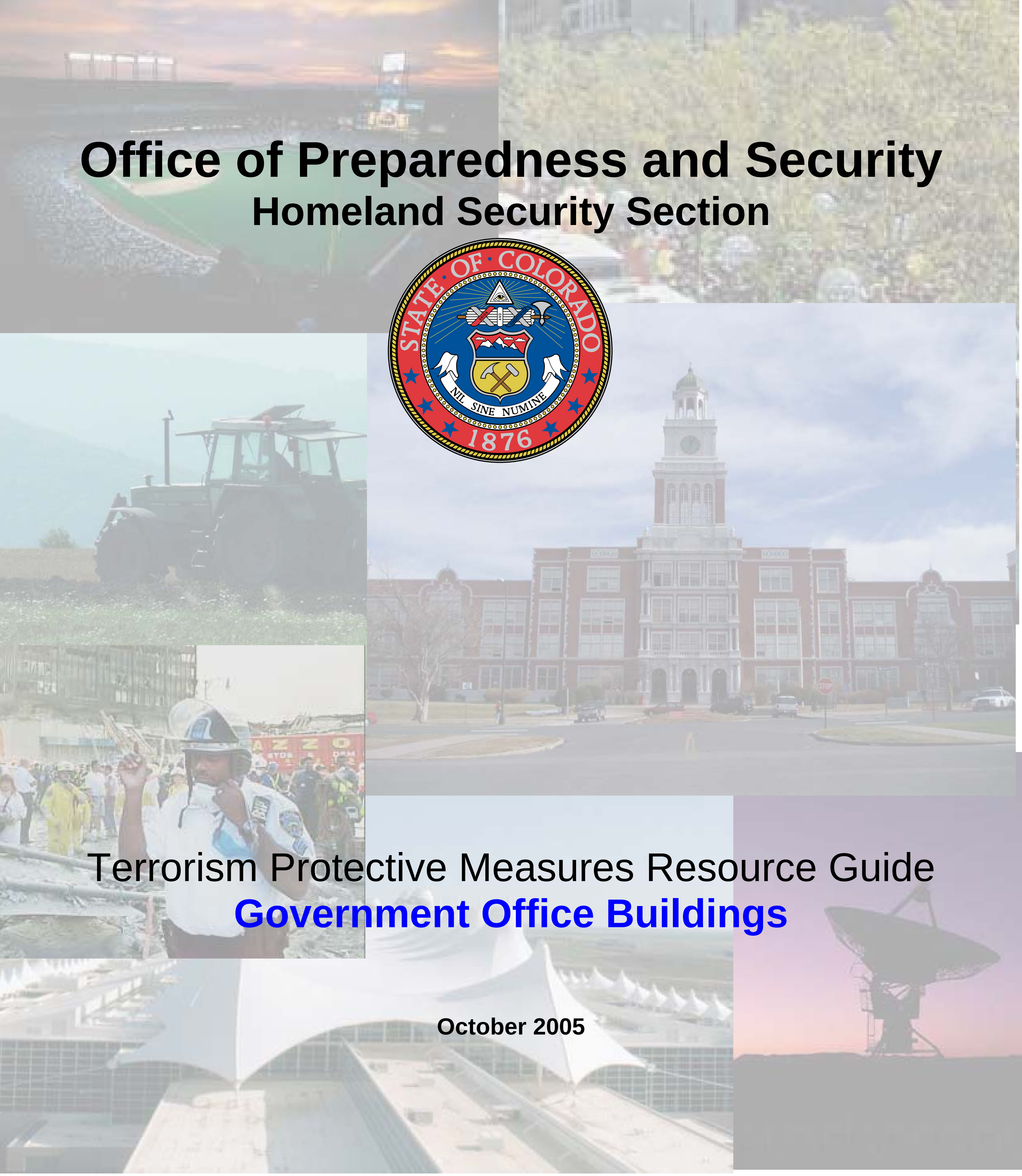


Office of Preparedness and Security

Homeland Security Section

Terrorism Protective Measures Resource Guide

Government Office Buildings

October 2005

The purpose of this guide is to give an overview of the terrorist threats that face our state and measures we can take to protect ourselves. It is one of our missions at the Office of Preparedness and Security, Homeland Security Section, to work with the many communities within our state with the common goal of protecting our citizens, critical infrastructures, and the assets they control. This guide is intended to give information that can assist in determining areas within your facility that are vulnerable to possible terrorist attacks and ways in which to protect them.

Protective measures are employed in order to:

- Increase awareness among site managers and law enforcement
- Reduce vulnerabilities of sites and their respective critical assets, and/or
- Enhance the defense against and response to an attack

This guide establishes an overview of; terrorist objectives, gives examples of specific threat categories, available protective measures, implementation of protective measures, and a protective measures matrix.

The Office of Preparedness and Security also maintains a specialized team (Team Rubicon) that provides on site vulnerability assessments. The team will provide subject matter expertise to prevent loss or disruption of critical infrastructure, key assets and key resources as a result of terrorist actions, natural disasters, and criminal activities. The results of the assessment are confidential and exempt from the Colorado open records law. The results are provided only to the site.

Please contact OPS at (720) 852-6720 or ops@cdps.state.co.us to obtain more information on this service and to schedule an assessment.

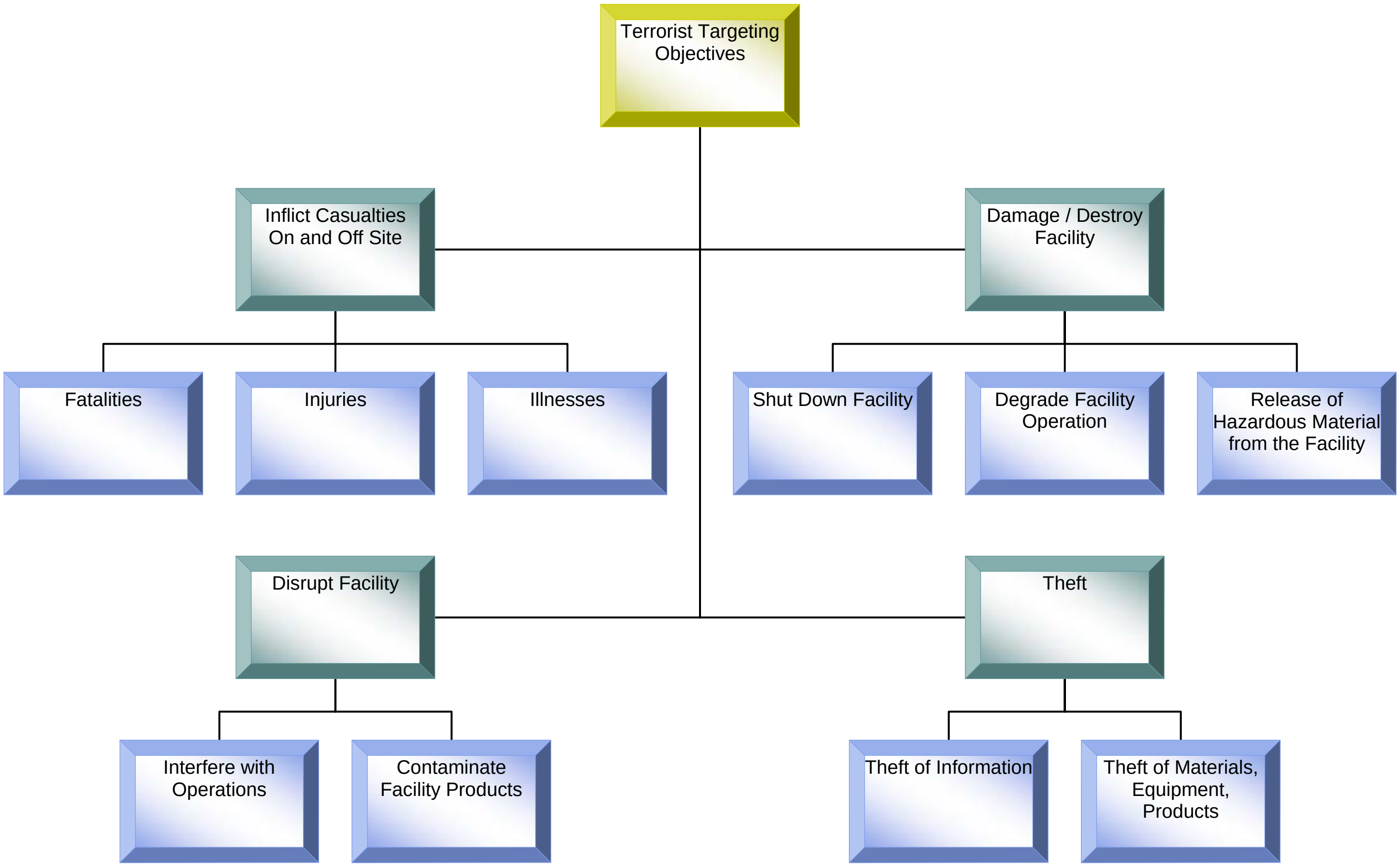
There are thirteen critical infrastructure sectors and four key resource segments. While a number of protective measures can be implemented for any of the thirteen critical infrastructure sectors, this guide is customized with protective measures for the following sector:

Infrastructure: Government Office Buildings

Terrorist Objectives

In general terms, terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States in order to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence. Figure 1 depicts the range of possible objectives for a terrorist attack on government office buildings.

Figure 1


Terrorist Targeting Objectives
Inflict Casualties On and Off Site
Damage / Destroy Facility
Fatalities
Injuries
Illnesses
Shut Down Facility
Degrade Facility Operation
Release of Hazardous Material from the Facility
Disrupt Facility
Theft
Interfere with Operations
Contaminate Facility Products
Theft of Information
Theft of Materials, Equipment, Products

Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many terrorist acts. Casualties can occur both at a targeted facility and in the surrounding area.

Damage or destruction of the facility can be intended to shut down or degrade the operation of the facility or to cause the release of hazardous materials to the surrounding area. Disruption of the targeted site without inflicting actual damage can be intended to interfere with the facility operations and cause a decrease of output or to tamper with the facility products to render them dangerous and/or unstable.

Theft of equipment, materials, or products can be intended to divert these items to other uses to reap financial gain from their resale. Theft of information can be intended either to acquire insight that is not public information or to gain data that can be used to carry out attacks.

Threat categories

Terrorists have a variety of weapons and tactics available to achieve their objectives and have demonstrated the ability to plan and conduct complex attacks, simultaneously, against multiple targets. Attacks can be carried out by individuals, small teams of a few perpetrators, or larger groups acting in a coordinated fashion. Some of the many potential categories of threats of concern are described in the following sections.

Improvised Explosive Devices (IEDs)

Explosives are a common weapon employed by terrorists. They range from small explosive devices detonated by a lone suicide bomber to large quantities of explosives packed into a car, truck or waterborne craft. There have been an increasing number of coordinated bombing attacks around the world.

Chemical Attack

Chemicals can be exploited or used by terrorists as a weapon. Such chemicals include toxic industrial chemicals (e.g., chlorine, ammonia, hydrogen fluoride) and chemical warfare agents (e.g., sarin gas, VX gas).

Biological Attack

Biological pathogens (e.g., anthrax, botulin, plague) can cause disease and are attractive to terrorists because of the potential for mass casualties and the exhaustion of response resources.

Nuclear/Radiological attack

Although weapons-grade nuclear material is relatively difficult to obtain, some sources of nuclear and radiological material are more readily available (e.g., from medical diagnostic equipment) and easier to deliver than others in the form of a radiological dispersal device.

Aircraft Attack

Both commercial and general aviation aircraft can be used to deliver attackers, explosives, or hazardous materials; they can also be used as weapons in and of themselves.

Maritime Attack

Boats of various sizes can be used to deliver attackers, explosives, or hazardous materials; they can also be used as weapons in and of themselves.

Cyber Attack

Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Supervisory control and data acquisition systems can be infiltrated to operate infrastructure systems in order to cause damage and inflict on-site and off-site casualties.

Sabotage

The distribution, damage, or destruction of a facility through sabotage, the introduction of hazardous materials into the facility, and/or contamination of facility products is of concern. In some cases, sabotage is designed to release hazardous material from a facility into the surrounding area.

Assassination/Kidnapping

Assassinating key personnel or kidnapping individuals and taking hostages has been used in many terrorist acts.

Small Arms Assaults

Small arms, including automatic rifles, grenade launchers, shoulder fired missiles, and other such weaponry, can be aimed at people (e.g., shooting of civilians) or at facilities (e.g., stand-off assault from outside a perimeter fence).

Available Protective Measures

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

Devalue	Lower the value 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 effectively respond.
Deter	Make the facility more difficult to attack successfully.
Defend	Respond to an attack to defeat adversaries, protect the facility, and mitigate any effect of an attack.

Many different protective measures are available for deployment at a facility and in the areas around it. Some are applicable to a wide range of facilities and against a number of threats, while others are designed to meet the unique needs of a specific facility or a specific threat. In addition, some may be tactical in nature, while others may address long-term strategic needs.

In general, applicable protective measures can be grouped into several broad categories as shown in table 1 on the following two pages. The table is intended to be illustrative rather than comprehensive. In addition to these generally applicable measures, some protective measures that are specifically orientated toward the Government Office Buildings are given at the end of this guide in the Protective Measure Matrix.

Available Protective Measures Matrix

Protective Measures and Type	Protective Measures Description and Examples
Access Control	**Control of employees/visits/vehicles entering a facility site or a controlled area in the vicinity of a facility**
	Controlled entrances (e.g., doors, entryways, gates, locks, turnstiles, door alarms)
	Control of material (e.g., raw materials, finished product)
	Secure perimeters (e.g., fences, bollards)
	Restricted access areas (e.g., key assets, roofs, heating, ventilation, and air conditioning
	Access identification (e.g., employee badges, biometric identification
	Signage
Barriers	**Physical barriers and barricades**
	Walls
	Fences (e.g., barbed wire, chain link)
	Earth banks and berms (e.g., for blast protection)
	Screens and shields (e.g., for visual screening)
	Vehicle barriers (e.g., bollards, jersey barriers, planters, vehicles used as temporary barriers)
Monitoring and Surveillance	**Use of equipment to monitor movements of people and material in and around a facility and to detect contraband**
	Closed-circuit television, cameras (e.g., fixed, panning, recording capability)
	Motion detectors
	Fire and smoke detectors
	Heat sensors
	Explosive detectors
	Chemical agent detectors
	Biological agent detectors
	Radiological agent detectors
	Metal detectors
	Night-vision optics (infrared, thermal)
	Lighting (buildings, perimeter, permanent/temporary
Communications	**Communication capability within a facility and between a facility and local authorities**
	Telephone (land line, cell, satellite)
	Radio
	Interoperable equipment (within facility, with local jurisdictions)
	Redundant and backup communication capabilities
	Data lines (internet, perimeter, permanent, temporary)
Inspection	**Inspection of people, vehicles, and shipments for explosives, chemical/biological/radiological agents**
	Personnel searches (including employees, visitors, contractors, vendors)
	Vehicle searches (cars, trucks, delivery vehicles, boats)
	Cargo and shipment searches
	Trained and certified dogs
	X-ray screening
	(Continued on following page.)

Protective Measures and Type	Protective Measures Description and Examples
Security Force	**Personnel assigned security responsibility**
	Force size
	Equipment (weapons, communication gear, vehicles, protective clothing and gear, specialized incident-response gear)
	Training
	Operational procedures (patrols, checkpoints, local law enforcement, state police, FBI, National Guard)
	Coordination among facility force, local law enforcement, state police, FBI, National Guard
Cyber Security	**Protection of computer and data systems**
	Firewalls
	Virus protection
	Password procedures
	Information encryption
	Computer access control
	Intrusion detection systems
	Redundant and backup systems
Security Program	**Procedures and policies**
	Employee background checks
	Employee security awareness and training
	Visitor control and monitoring
	Security reporting system
	Operations security plan
	Coordination among facility, local law enforcement, state and federal agencies,
Incident Response	**Procedures and capability to respond to an attack**
	Emergency response plan
	Emergency response equipment
	Emergency response personnel
	Emergency response training and drills
	Shelter facilities
	Communication with public
Personnel Protection	**Procedures to protect personnel from attack**
	Protection for high-profile management personnel (e.g., guard escorts, schedule and route changes)
	Protection for employees (e.g., alerts, reduced travel and business activity outside facility)
Infrastructure Interdependencies	**Protection of site utilities, material inputs, and products**
	Utilities (e.g., electric power, natural gas, petroleum products, water, telecommunications)
	Inputs (e.g., raw materials, parts)
	Outputs (e.g., finished products, intermediate products)

Implementation of Protection Measures

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

The implementation of any protective measure at any time involves the commitment of resources in the form of people, equipment, materials, time and money. Facility owners, local law enforcement, emergency responders, and state and local government agencies need to coordinate and cooperate on what measures to implement, how extensive they should be, and how long they should be kept in force in order to maximize security while staying within the bounds of available resources.

To assist in the decision process, the U.S. Department of Homeland Security has developed the color-coded Homeland Security Advisory System (HSAS) to communicate with public safety officials and the public at large so that protective measures can be implemented or expanded to reduce the likelihood or impact of an attack. Table 2 shows the HSAS.

Alert Level		Description
Red	SEVERE	Severe Risk of Terrorist Attack
Orange	HIGH	High Risk of Terrorist Attack
Yellow	ELEVATED	Significant Risk of Terrorist Attack
Blue	GUARDED	General Risk of Terrorist Attack
Green	LOW	Low Risk of Terrorist Attack

When the available intelligence allows, the HSAS alerts are supplemented by information on a threat most likely to be used by terrorists. This information may or may not be very specific in regards to area or time of an attack. 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.

Random Anti-Terrorism Measures

While the best protection can be obtained by implementing all proposed protective measures, in some cases it may not be feasible to implement every protective measure 100% of the time due to financial or manpower restraints. Studies have shown an alternative method of randomizing measures may also be effective. For instance, every day a security measure is implemented for half the day. On the first day the local police department is brought in to walk an explosive detecting dog around the facility. Later in the day, all personnel are stopped from entering until a photo ID can be checked. The next day every fifth vehicle is searched when driving into the parking lot. These methods are changed daily, disrupting a critical piece of the terrorism event planning. While terrorists are surveilling possible targets, they observe security measures in place. By frequently changing the security measures, the target is made less attractive due to the unpredictable nature of these random ant-terrorism measures.

Protective Measures

The following Exhibits1-5 are designed to provide information and assistance to facility owners, local law enforcement, and state and local homeland security agents in making decisions on how to increase security measures on the basis of HSAS alert levels. These suggested measures are collated from infrastructure-specific guidance and from experience in a number of localities across the country. The following should be noted regarding the suggested measures:

These suggestions are intended as a guide; they are not a requirement under any regulation or legislation.

The suggested steps are additive in that higher levels should also include those measures outlined for lower threat levels.

These suggestions are based on practices employed by facilities across the nation. The ability to implement them at any specific facility will vary.

These suggestions should not be viewed as a complete source of information on protecting your facility. Facility managers and local security personnel should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

These guides are not intended to supersede any existing plan or procedures, but are intended to work with or be implemented with current plans and procedures.

Exhibit 1 Protective Measures Implemented at HSAS Threat Level Green

Measures put in place under this threat level can be considered to be "baseline countermeasures" that are in place under all conditions. Industry-developed guidelines provide detailed information on specific measures (see Pages 5-9), which are not repeated here. The following list provides a brief summary of the major types of measures suggested by industry organizations for implementation.

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
	X	X		Validate that existing security access control measures (e.g., locks, door alarms, card access devices) are in good working order.	
	X	X		Identify those measures and resources that can enhance security at higher threat condition levels.	
	X	X		Control access to all key command, control, and communications areas and other critical facilities at all times.	
	X	X		Maintain awareness of any contractors who are working on a critical facility (e.g., HVAC, fire alarms).	
	X	X		Develop plans for restricting vehicular access.	
				Barriers	
		X	X	Ensure that existing fencing is functional.	
		X	X	Work with law enforcement to develop a vehicle parking plan that provides safe-distance parking next to and around facilities, including garages or underground/under-building parking.	
				Monitoring and Surveillance	
	X			Survey surrounding areas to determine how threats to neighboring facilities (e.g., airports, government buildings, industrial facilities, railways, electric power lines, shipping vessels/waterways) could affect the facility.	
	X	X		Provide adequate lighting in security areas.	
	X	X		Provide video surveillance systems for the critical areas and connect the systems to a central monitoring control room.	
	X			Advise all personnel to report the presence of unknown persons, unidentified vehicles, vehicles parked in an unusual manner, abandoned parcels or packages, and other suspicious activities.	
				Communications	
	X	X		Maintain and monitor building communications and warning systems.	
	X	X	X	Develop liaison with local law enforcement emergency response teams to enhance information exchange, clarify emergency response, track threat conditions, develop communications methods and alternatives, and support investigations.	
			X	Provide names and phone numbers for key contact personnel to the emergency response organizations.	
			X	Develop canned messages that can be disseminated to the workforce at the announcement of various threat levels. Determine when, by whom, and how those messages will be disseminated.	
				Inspection	
	X	X		Conduct routine security inspections.	
				Security Force	
X	X	X	X	Maintain an adequately staffed and equipped security force.	
X	X	X	X	Conduct regular patrols of facility using a random time schedule.	
X	X	X	X	Train security personnel on acceptable and appropriate responses to civil disturbances, demonstrations, protests, and other such situations.	
				Cyber Security	
		X	X	Determine the threats to existing/proposed information technologies. Conduct cyber asset classification to identify assets that require protection.	
	X	X	X	Establish an information/data security risk management program. Develop and implement hardware, software, and communication security for computer-based operational systems.	
		X	X	Implement cyber access controls, including (1) administrative controls (e.g., policy, procedures, training, background checks, and supervision) and (2) logical or technical controls to restrict access to systems and information (e.g., passwords, tokens, encryption, system hardening, and protected protocols).	
X		X	X	Control access to information technology systems (on-site, remote access).	
	X	X		Log and monitor for inappropriate network activities.	
	X	X		Install antivirus software throughout the enterprise on personal computers, data file servers, and centralized applications servers and in the firewall complex.	
	X	X		Define the network security perimeter by appropriately configured and managed control devices, such as security gateways and firewalls. (Cont.)	

Exhibit 1 Protective Measures Implemented at HSAS Threat Level Green

Measures put in place under this threat level can be considered to be "baseline countermeasures" that are in place under all conditions. Industry-developed guidelines provide detailed information on specific measures (see Pages 5-9), which are not repeated here. The following list provides a brief summary of the major types of measures suggested by industry organizations for implementation.

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
		X		Review and thoroughly test applications that require processing of sensitive data before putting them into production, and periodically reevaluate them to ensure application integrity is maintained.	
	X	X		Create an information technology security education and awareness program for technical administrators and key focal points.	
	X	X		Establish a comprehensive employee training program that addresses information/data security.	
				Security Program	
X	X	X	X	Develop a comprehensive security plan, policies, and procedures.	
	X	X		Conduct employee background screening.	
	X	X		Screen contractors, temporary employees, and visitors.	
	X	X	X	Conduct regular security audits.	
X	X	X		Caution employees not to talk with outsiders about their facility or related topics.	
X	X	X		Develop a terrorism and security awareness program, and educate and train employees and specified contractor personnel on security standards and procedures.	
	X		X	Review and validate procedures for heightened alert status.	
X		X		Review information posted to Web sites and be prepared to remove it if it compromises security.	
			X	Develop emergency procedures and training for people with special needs.	
	X		X	Be cognizant of current events. Monitor television, radio, and newspaper reports.	
	X	X	X	Prepare and review risk assessments performed against facilities, assets, and personnel.	
				Incident Response	
X			X	Develop emergency operations and business continuity-of-operations plans that address such topics as readiness, prevention, response, recovery/resumption, testing and training, and evaluation and maintenance.	
			X	Maintain an adequately staffed, equipped, and trained emergency response team.	
			X	Develop a communications plan for emergency response and notification of key personnel.	
			X	Conduct drills and exercises for emergency response team and facility occupants.	
	X	X	X	Capture "lessons learned" after each incident or exercise.	
			X	Develop procedures for shutting down and evacuating the facility. Facilities located near critical community assets should be especially vigilant.	
			X	Prepare for the possibility of flooding or other destruction as a result of a bombing incident or other similar catastrophic events.	
			X	Establish liaison/working relationships with emergency management and first responders.	
			X	Ensure that local agencies are familiar with the physical layout and operational procedures. Designate arrival location for emergency response vehicles.	
				Personnel Protection	
			X	Consult with local first responders and other government agencies regarding best actions to develop relative to "shelter in place"	
	X		X	Encourage and assist employees and their families to be prepared for personal, natural, technological, and homeland security emergencies.	
				Infrastructure Interdependencies	
			X	Know how to turn off power, gas, and water. Ensure procedures are ready for dealing with emergency shutdowns of HVAC systems in the event of a possible internal or external chemical release.	
		X	X	Prepare contingency plans for loss of critical utility services (water and electric power).	
		X	X	Ensure coordination with supporting telecommunication restoration priorities and plans.	

Exhibit 2 Protective Measures Implemented at HSAS Threat Level yellow

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
		X		Review security hardware on doors, locks, and windows. Check emergency exit doors for functionality and operation.	
	X	X		Ensure adequate access control measures and procedures; enhance as needed, especially at critical facilities.	
		X	X	Reduce the number of access points, if possible, for vehicles and personnel, and periodically spot check the contents of vehicles.	
	X	X		Use company-issued or government-issued photo IDs.	
	X	X		Require visitors to check in at facility office to verify their identification. Be especially alert with regard to repeat visitors or outsiders who have no apparent business at the facility and are asking questions about the facility or its personnel.	
	X	X	X	Install emergency buzzers from dock ingress and egress to central command center.	
				Barriers	
		X	X	Work with law enforcement to develop plans for installing barriers (e.g., large flower pots, cement stanchions) to prevent vehicles from driving through the facility entrance doors/gates.	
				Monitoring and Surveillance	
	X			Check operation of CCTV systems and review policies with facility personnel.	
	X	X		Install (or verify operation of) duress alarms to the central command center from the reception desk and/or remote guard stations, executive offices, and key access points.	
	X	X		Upgrade surveillance cameras and alarm systems, if appropriate, for heightened threat levels.	
	X			At regular intervals, remind all personnel to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of the facility. Watch for abandoned parcels or suitcases or any unusual activity.	
				Communications	
	X	X	X	Inform personnel of a change in alert status.	
	X	X	X	Review with employees the operations plan, personnel safety, security details, and logistic requirements that pertain to the increased security level.	
	X	X	X	Review all data and voice communication channels to ensure operability, user familiarity, and back-up functions as designed.	
	X	X	X	Ensure that telephone and radio/phone contact with local law enforcement works.	
		X	X	Test emergency communication procedures and protocols.	
		X	X	Plan for alternate means of communication if phone lines are not available. Determine availability of satellite capability to support communications if cell phone reception is not available.	
				Inspection	
	X	X		Increase frequency of inspections and patrols within facilities, including, the interior of the buildings and along their perimeter.	
	X	X		Develop procedures to inspect items carried into the facility by personnel, contractors, and visitors.	
	X	X	X	Review the U.S. Postal Service (USPS) “Suspicious Mail Alert” and “Bombs by Mail” publications with all personnel involved in receiving packages.	
				Security Force	
	X	X	X	Review and verify availability of additional/back-up personnel to support security and facility functions.	
				Cyber Security	
	X			Increase monitoring of all external network connections.	
		X	X	Increase the frequency of mission-critical data back-up.	
	X	X	X	Review and validate information/data security response plan, if established.	
	X	X		Refresh employees’ knowledge of social engineering techniques designed to trick employees into divulging information that could be used to compromise data security.	

Exhibit 2 Protective Measures Implemented at HSAS Threat Level yellow

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Security Program	
	X	X	X	Review all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.	
	X	X	X	Review budgets that support required security measures as costs increase due to heightened threat level. Determine if partnerships can be leveraged with other organizations to reduce costs.	
	X	X	X	Develop tabletop exercises of procedures that may be appropriate.	
		X	X	Establish a process for periodic monitoring of television, radio, and news reports, and incorporate this capability in the central command center.	
	X	X	X	Review, update, and routinely exercise security plans.	
	X	X	X	Review physical security precautions.	
	X	X		Review provisions for employee picture ID badges and background checks.	
				Incident Response	
	X	X	X	Review contingency and evacuation/relocation plans and emergency response manuals.	
			X	Establish a crisis management team and other related response teams, such as an emergency response team, incident response team, and disaster recovery team, and train them with regard to their responsibilities for each threat level.	
		X	X	Review and update the call-down list for emergency response teams.	
			X	Inventory and verify the readiness of protective equipment, if available.	
			X	Review and validate that basic training of response personnel is current and adequate with regard to possible threat conditions relevant to the organization.	
			X	Ensure that the organization's first responders are certified in first aid, cardiopulmonary resuscitation (CPR), and the use of automatic external defibrillators (AEDs).	
		X	X	Develop relationships and documents (memorandums of understanding and agreement [MOUs, MOAs]) if appropriate, with local, state, and federal agencies, including emergency management, law enforcement, and the military. Determine if partnerships can be leveraged with other organizations to reduce costs.	
	X	X	X	Invite local fire, police, emergency medical service (EMS), and regulatory agencies to training exercises designed for the organization's crisis management team and related response teams.	
				Personnel Protection	
	X	X		Reinforce personal security awareness.	
	X	X	X	Give key personnel, vendors, suppliers, and contractors a copy of the facility emergency procedures and other pertinent organizational guidelines.	
				Infrastructure Interdependencies	
			X	Maintain independent emergency telephone lines separate from facility private branch exchange (PBX). In addition, develop back-up/alternate methods of communication.	

Exhibit 3 Protective Measures Implemented at HSAS Threat Level yellow

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
X				Consider removing or covering government agency logos.	
	X	X		Perform housekeeping of exterior grounds of facilities, limiting the storage of items (e.g., crates, other objects) that would provide camouflage.	
	X	X	X	Enhance or provide manned coverage of dock areas, if not already doing so.	
	X	X		Verify truck driver's license, bills of lading, and other applicable paperwork relative to deliveries.	
X			X	Validate all building alarm's, access controls, intrusion detection systems, and building systems in accordance with threat conditions.	
		X		Close and lock all gates and barriers, except those needed for immediate entry/egress.	
	X	X		Assign personnel to assist with security duties, monitoring personnel entering the facility, inspecting the area on a regular basis, and reporting to the facility management as issues surface.	
				Barriers	
		X	X	Install jersey barriers to prevent vehicles from entering or nearing critical facilities.	
		X	X	Install tire shredders at critical entrances.	
				Monitoring and Surveillance	
	X			Review the list of individuals notified by automatic alerts generated by security monitoring systems (e.g., network and information technology intrusion detection systems).	
	X	X		At beginning and end of each work day, inspect interior/exterior of buildings and storage areas in regular use. Inspect all vulnerable areas in critical facilities.	
	X	X		Increase building spot checks.	
	X	X		Check HVAC filtration; any detectors, monitors, or alarm systems; and water system security.	
	X	X		Ensure that other security systems are functioning and available for use.	
				Communications	
	X	X	X	Inform personnel of the change in alert status.	
	X	X	X	Review with employees operations plans, personnel safety, security details, and logistic requirements that pertain to the security level.	
	X	X	X	Ensure that all telephone, radio, and satellite communication systems are in place with all concerned personnel.	
	X	X	X	Enhance interface with law enforcement, safety, and related emergency responder groups.	
		X		Implement procedures to provide periodic updates to employees on security measures being implemented.	
		X	X	Verify that all cell phones and pagers are ready for distribution to the members of the crisis management team and related response teams.	
		X	X	Determine if cell phones should have text messaging capability.	
		X	X	Ensure that communication channels and processes are open, reliable, and consistent and that alternative/back-up forms of communication are available.	
				Inspection	
	X			Review and verify vehicle inspection training for security personnel.	
	X	X		Physically inspect cargo as necessary.	
	X	X		Consider increasing screening activity of inbound packages.	
	X	X		Raise awareness regarding delivery of suspect mail and packages.	
	X			Enhance mail inspection procedures.	
				Security Force	
	X	X	X	Consider guard reinforcement and ensure that all guards are adequately trained in company procedures.	
				Cyber Security	
	X	X	X	Increase review of intrusion detection and firewall logs.	
		X		Perform penetration testing of individual organizational sites and encourage participation by vendors to validate cyber security levels.	
	X	X		Refresh employees' knowledge of the danger of malicious code delivered by e-mail via worm, viruses, etc…	
				Security Program	
		X		Announce Threat Condition Yellow – Elevated.	
X	X	X		Review vulnerability and threat assessments and revise as needed.	
		X		Update and test call-down lists for emergency response teams and key employees. (Cont.)	

Exhibit 3 Protective Measures Implemented at HSAS Threat Level yellow

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
X	X	X		Review, coordinate, and update mutual aid agreements with other critical facilities and government agencies.	
	X	X		Establish and monitor active and passive security measures.	
	X	X		Review employee training on security precautions (bomb threat, procedures, suspicious mail-handling procedures, etc.).	
	X	X	X	Verify the equipment, communications lists, and processes in the central command center, if established.	
		X	X	Verify contacts and communicate with the law enforcement community and local outside emergency medical, fire, and response personnel.	
	X	X		Obtain threat and intelligence updates from local, state, and federal authorities as well as private industry security sources.	
	X	X		Ensure security-related information is communicated to personnel across the organization, as approved by leadership.	
	X	X		Periodically review actions taken to date against the stated threat conditions, since they may rapidly change for better or worse.	
	X	X		Maintain a high level of suspicion and remain alert to unusual activities, occurrences, and behavior.	
				Incident Response	
	X	X	X	Review and refine emergency response processes within the context of the current threat information.	
			X	Ensure that a response can be mobilized as appropriate for the increased security level.	
			X	Review communication procedures and back-up plans with all concerned personnel.	
		X	X	Ensure that all business, emergency, and continuity/recovery plan documents (e.g., contact lists, notification/escalation procedures) are up to date.	
			X	Convene crisis management team and other related response teams to review emergency response and business continuity/recovery plans. Confirm functional responsibilities.	
				Personnel Protection	
	X	X		Emphasize and elevate the importance of knowing about planned absences, arrivals, and whereabouts of all personnel.	
		X	X	Increase the frequency of warnings required under lower threat conditions. Inform personnel of additional threat information as available.	
		X	X	Provide periodic updates on security measures being implemented.	
		X	X	As appropriate, review with the facility employees the operations plans, security details, personnel safety, and logistics requirements that pertain to implementing increased security levels.	
				Infrastructure Interdependencies	
	X	X		Increase inspection of infrastructure connection points (e.g., electric power, telecommunications, water, natural gas).	

Exhibit 4 Protective Measures Implemented at HSAS Threat Level Orange

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
	X	X		Evaluate requiring special identification for day labor (e.g., special badges, colored wristbands). Inspect government-issued photo ID as proof of identification each time.	
		X		Strictly enforce access control to all critical facilities, especially control rooms.	
		X		Restrict vehicle parking close to buildings.	
	X	X	X	Evaluate arranging for security or law enforcement vehicles to be parked randomly near access points and exits.	
	X	X		Prepare to restrict access to essential personnel only.	
		X		Limit driveway and parking area access as appropriate.	
		X		If feasible, discontinue, limit, or otherwise control inside perimeter parking.	
		X		Evaluate eliminating underground parking.	
		X		If permissible, in compliance with fire code, restrict access to rooftops or, at a minimum, monitor continuously.	
		X		Reduce the number of access points for vehicles and personnel to minimum levels.	
		X		Evaluate restricting services provided by outside vendors/suppliers (e.g., cleaning crews) to possible nonessential site visits.	
		X		Validate vendor lists for all routine deliveries and repair services.	
		X		Discontinue tours and cease other nonessential site visits.	
				Barriers	
		X	X	Erect barriers and obstacles to control vehicle traffic flow and protect the facility from attack by a parked or moving vehicle. Consider using agency vehicles for this purpose.	
		X		Review all outstanding maintenance and capital project work that could affect the security of facilities.	
				Monitoring and Surveillance	
X	X	X		Assign additional staff in the central command center to monitor existing security cameras in real time.	
	X	X		Evaluate the use of special foot patrols, bicycle patrols, etc… Use canine patrols if appropriate.	
	X	X		Install temporary CCTV at potential surveillance points, administration buildings, docks, and control room access points.	
	X	X		Enhance visibility in and around perimeters by increasing lighting and removing or trimming vegetation.	
	X	X		If conditions warrant, conduct heightened screening of all inbound mail. Direct attention to any packages or letters received without a return address or having indications of stains/powder.	
				Communications	
	X	X	X	Include security and awareness briefings as part of daily job briefings.	
				Inspection	
	X	X		Check and screen all deliveries.	
	X	X		Increase the frequency of random briefcase and carryall inspections.	
	X	X		Search all vehicles and contents before they enter the facility.	
	X	X		Search all personnel bags and parcels, and require personnel to pass through security checkpoints.	
	X	X		Inspect all deliveries and consider accepting shipments only at off-site locations.	
	X	X		Evaluate vehicle inspection program to include checking beneath the undercarriage, under the hood, and in the trunk of vehicles.	
	X	X	X	Approach all illegally parked vehicles in and around facilities. Question drivers and direct them to move immediately. If owner cannot be identified, have the vehicle towed.	
	X	X		Increase inspections in and around the facility to ensure that utility and emergency systems are not tampered with, damaged, or sabotaged. The effort should include emergency generation and lighting, fire alarms, and perimeter protection.	
	X	X	X	Implement frequent inspection of critical facilities, including the exteriors and roofs of all buildings and parking areas. (Cont.)	

Exhibit 4 Protective Measures Implemented at HSAS Threat Level Orange

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
	X	X	X	Increase patrolling at night to ensure that all vulnerable critical points are fully illuminated and secure.	
	X	X		Check all security systems, such as lighting and intruder alarms, to ensure that they are functioning.	
	X	X		Modify lighting levels, as appropriate, to address changing security needs.	
	X	X		Assign personnel at facility to assist with security duties by monitoring personnel entering the facility, checking vehicles entering the facility, patrolling the area regularly, and reporting to facility management as issues surface.	
	X	X		Resurvey the surrounding area to determine whether activities near a critical facility (e.g., airports, government buildings, industrial facilities, railroads, waterways, etc…) could create hazards that could affect the facility.	
	X	X		Increase inspections on building systems and infrastructure, including HVAC systems.	
	X	X		Inspect and, if feasible, secure vacant rooms (e.g., meeting, guest, housekeeping, storage rooms).	
				Security Force	
	X	X	X	Increase numbers of security guards and patrol activities.	
	X	X		Determine increased officer requirements for extended periods. Possibly suspend holidays, etc…, and hold discussions with contract security providers for increased human resources.	
		X		Implement random shift changes of security guards.	
				Cyber Security	
X		X		Evaluate publicly accessible Web sites, and, where necessary, close down nonessential services. For remaining sites, ensure that all operating systems and related application software patches are applied.	
		X		Ensure organizational security specialists have reviewed the organization’s security definition for currency.	
	X			Enhance monitoring of activity on essential services for publicly accessible Web sites to identify deviations from normal activity.	
		X	X	Implement more frequent back-up procedures.	
	X	X	X	Conduct immediate internal security review of all critical systems.	
	X			Enhance monitoring of logging and intrusion detection for remaining sites, and review reporting mechanisms that are linked to an intrusion alert and notification system.	
		X		Consider delaying scheduled, routine maintenance, or non-security-sensitive upgrades.	
X		X		Validate distributed denial-of-service preparedness, and check with Internet service provider regarding its ability to help (e.g., block address ranges).	
				Security Program	
		X	X	Announce Threat Condition Orange – HIGH	
		X	X	Place all critical and on-call personnel on alert.	
		X	X	Place emergency response teams on notice.	
	X	X	X	Activate the business emergency operations center if required.	
	X	X	X	Ensure the appropriate security measures are in place and functioning properly.	
	X	X	X	Instruct personnel to immediately report suspicious activity, packages/articles, people, and vehicles to security personnel. Call 9-1-1 for immediate response, if needed.	
	X	X		Be cognizant of unattended packages/articles and vehicles.	
	X	X	X	Move automobiles and other non-stationary items at least 30 yards from the facility, particularly buildings and sensitive areas, unless doing so would create a safety hazard or impede other security measures.	
	X	X	X	Identify areas where explosive devices could be hidden and arranged for regular inspection.	
X	X	X		Cancel or delay all non-vital facility work conducted by contractors, or have company personnel continuously monitor the contractor’s work.	
	X	X		Discuss and coordinate with facilities and building management other security controls for guests and vendors.	
		X	X	If elevators are on premises, train staff in the operation of the elevators and the correct response in the event of an emergency.	
			X	Coordinate operations related to critical infrastructure concerns with armed forces (i.e., armed security, local law enforcement, or the military).	
		X	X	Staff central command center, if in existence, during normal operational hours and continue to review call lists for currency. (Cont.)	

Exhibit 4 Protective Measures Implemented at HSAS Threat Level Orange

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher level alert levels to determine which measures should be implemented on the basis of the current threat and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
		X	X	Run call tests and verify that all equipment is operational.	
				Incident Response	
	X	X	X	Implement emergency and contingency plans as necessary.	
	X		X	Ensure that all personnel responsible for implementing countermeasures are immediately available. Staff critical facilities where feasible.	
		X	X	Convene emergency response/crisis management teams to review the more specific information that is available from law enforcement, the media, and other sources to assess the potential impact to the organization.	
			X	Provide cell phones and pagers to the members of the crisis management team and related response teams, if not already done.	
X			X	Verify that alternate locations are valid and that personnel supporting recovery operations are current in their obligations.	
			X	Prepare for possible evacuation, closing, and securing of all individual organization facilities.	
			X	Review the ability of the facilities and building management to rapidly shut down HVAC equipment. Discuss conditions whereby HVAC is to be shut down and restarted.	
				Personnel Protection	
	X	X		Update personnel on escalating threat.	
			X	Verify shelter-in-place procedures and equipment.	
			X	Ensure that best available filtration is being used for existing HVAC configuration.	
				Infrastructure Interdependencies	
		X	X	Review plans to address any redirection or constraint to transportation systems.	
		X	X	Consult with local authorities about control of public roads and accesses that might make the facility more vulnerable if they were to remain open.	

Exhibit 5 Protective Measures Implemented at HSAS Threat Level Red

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed, and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
X		X	X	Coordinate with local authorities regarding closing of public roads and facilities.	
X		X	X	Reduce facility access points to the absolute minimum necessary for continued operation.	
	X	X	X	Arrange to have heavy equipment placed at strategic locations near entrances and critical components.	
		X		Do not allow visitors.	
		X		Do not allow non-essential vehicles into critical areas.	
	X	X		Thoroughly search essential vehicles, including undercarriage and cab; enter cargo hold when possible.	
		X		Close or restrict entry to the facility to essential personnel only and restrict parking areas close to critical buildings.	
	X	X		Restrict or suspend all deliveries and mail to the facility. Send emergency supplies or essential shipments to an off-site location for inspection.	
		X		Stop non-essential contract services at the facility.	
		X		Staff all access points and restricted areas 24/7.	
	X	X		Restrict access to facilities, equipment, systems, and essential personnel only.	
				Barriers	
		X	X	Deploy temporary barriers at all key assets.	
				Monitoring and Surveillance	
		X	X	Establish surveillance points and returning criteria and procedures.	
	X	X		Make frequent checks of all facility exterior areas, including parking.	
	X	X		Enhance monitoring of all buildings and access control/intrusion detection systems (e.g., cameras, alarms, locks, lighting, and card access devices). Ensure frequent checks with other integrated security consoles.	
	X	X		Leave lighting on 24/7.	
	X	X	X	Increase security patrol activity at facility to the maximum levels sustainable.	
				Communications	
		X	X	Advise appropriate agencies that the facility is at Red level and provide advice as to the measures being used.	
			X	Test communications and notification procedures.	
			X	Advise site management of potential implementation of evacuation/relocation plan.	
			X	Conduct daily briefings with local law enforcement and industry information-sharing and coordination organizations on threat condition.	
			X	Request assistance form local police agencies to secure the facility and control access.	
			X	Cooperate with local police or other authorities if they direct security measures.	
		X	X	Extract and maintain a predetermined number of communication lines (telephone, fax, and Internet) for emergency purposes.	
				Inspection	
	X	X		Search all persons before they enter the facility.	
	X	X	X	Inspect all vehicles entering a facility, including the cargo areas, undercarriage, glove compartments, and other areas where dangerous items could be concealed.	
	X	X	X	Identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.	
	X	X		Utilize alternate, enhanced methods of inspection at designated access points.	
				Security Force	
	X	X	X	Augment security forces to ensure control of the facility and access to the facility and other potential target areas.	
X	X	X	X	Increase the number of security guards, guard postings, and roving guard visibility.	
		X	X	Augment security guards with law enforcement/military personnel where feasible. Have law enforcement officers on the site 24 hours per day as available.	
		X	X	Consider using armed guards.	
				Cyber Security	
		X	X	Restrict computer access to essential personnel only.	
		X	X	Increase computer security levels to maximum.	
X		X		If warranted, disconnect organization’s networks from the Internet.	
	X			Consider continuous 24/7 monitoring of cyber security communications for latest vulnerability information.	
			X	Contact software vendors for status of software patches and updates.	

Exhibit 5 Protective Measures Implemented at HSAS Threat Level Red

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed, and consider implementation of the following measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Security Program	
		X	X	Announce Threat Condition Red - SEVERE	
			X	Notify law enforcement of facility evacuation and closings.	
			X	Maintain close contact with local law enforcement and emergency management officials.	
X	X	X		Cancel or delay all non-vital facility work conducted by contractors, or continuously monitor their work with company personnel as applicable.	
X			X	Implement business contingency and continuity plans as appropriate.	
				Incident Response	
			X	Activate emergency response and continuity business plan for the critical facility.	
			X	Check all available emergency equipment.	
			X	Prepare emergency operations center for use.	
X			X	Prepare to work with a dispersed, or skeleton, crew of essential employees.	
			X	Implement business contingency and continuity plans as appropriate.	
X			X	Prepare to implement business recovery plans.	
			X	Deploy emergency response and security teams.	
			X	Convene emergency crisis management team and related response teams to manage and direct emergency response and/or business continuity/recovery plans in response to an imminent threat or actual event that impacts the organization, its employees, or third-party vendors/suppliers etc…	
			X	Operate the central command center, if in existence, and staff it fully 24/7.	
X			X	Prepare to close the facility, protect assets, and shut down equipment and systems in the event of an evacuation.	
			X	Assign the person or persons who, if anyone, will remain behind to protect and monitor the facility. Determine how and when facility will be reopened.	
X			X	Prepare to evacuate personnel and items as needed to support recovery operations.	
			X	Prepare for “manual evacuation” of essential computer hardware and systems, including support items needed for an alternate location of operations.	
			X	Check emergency supplies, restock if necessary, and place in a handy place.	
			X	Pre-position specially trained teams or emergency response personnel.	
			X	Redirect personnel to address critical emergency needs.	
				Personnel Protection	
	X	X		Update personnel on escalating threat.	
			X	Establish positive control on facility air intakes. Prevent all unfiltered air from reaching staffed spaces.	
			X	Ensure that guard force and shift supervisor/watch sections have breathing apparatus, if appropriate, and are prepared to evacuate or shelter-in-place.	
			X	Evacuate all non-essential personnel.	
X			X	Eliminate travel into an area affected by a terrorist attack or an area that is a target of an attack.	
X			X	Cancel attendance at non-critical or off-site meetings, conventions, symposia, etc…	
				Infrastructure Interdependencies	
			X	Implement plans to accommodate redirection or constraint of transportation.	

REFERENCES

1. Department of Homeland Security, Protective Security Division
"Protective Measures Infrastructures"
Information Guide
March 2005

2. DHS Protective Security Division
"Characteristics and Common Vulnerabilities, Infrastructure Category: Commercial Office Buildings"
June 2004

3. ASIS International
"Threat Advisory System Response Guideline"
(http://www.asisonline.org/guidelines/guidelinesthreat.pdf).

4. FEMA (Federal Emergency Management Agency), 2003
"Reference Manual to Mitigate Potential Terrorist Attacks against Buildings" FEMA 426
(http://www.fema.gov/pdf/fima/426/fema426.pdf)

5. Colorado Office of Preparedness, Security, and Fire Safety
"Threat Conditions Advisory System"
(http://www.ops.state.co.us/pdf/conditions.pdf)

RESOURCES

REFERENCE

http://www.mipt.org/ Oklahoma City National Memorial Institute to Prevent Terrorism
- http://www.mipt.org/First-Responders.asp Information for First Responders
- http://www.tkb.org/Home.jsp Terrorism Knowledge Base
- http://www1.rkb.mipt.org/ Responder Knowledge Base
- http://www.mipt.org/Building-Security.asp Information for Building/Facility managers

TRADE PUBLICATIONS

http://www.drj.com/ Industry magazine for disaster recovery, emergency management and business continuity
- http://www.drj.com/new2dr/newbies.htm special reference section for people new to the industry
- http://www.drj.com/new2dr/toolchest/drjtools.htm reference materials
- http://www.inptech.com/drj/login.php free subscription

http://www.disaster-resource.com/ general resource information, also has news alerts and articles
- http://www.disaster-resource.com/cgi-bin/freeguide.cgi free subscription to annual directory of suppliers

http://www.contingencyplanning.com/ industry magazine
- http://www.contingencyplanning.com/e-newsletters/index.aspxsubscribe to e newsletter
- http://www.contingencyplanning.com/archives/index.aspx reference to past articles

http://www.infosyssec.net/index.html information security
- http://infosyssec.tradepub.com/_brands/infosyssec/cat/Info.cat.html free publications for industry

http://www.disasterrecoverybooks.com/ books and reference materials

TRAINING/CERTIFICATION

http://www.drii.org/ offers training and professional certification for industry (non profit)
- http://www.drii.org/associations/1311/files/Course_Schedule.cfm schedule of online and field training

Colorado Office of Preparedness and Security Homeland Security Section
http://www.thebci.org/mainindex.htm offers training and professional certification for industry (non profit)

http://www.iaem.com/index.htm offers training and professional certification (non profit)

GOVERNMENT AGENCIES

http://www.fema.gov/

http://training.fema.gov/ Online and field training
http://training.fema.gov/EMIWeb/CERT/overview.asp Community Emergency Response Teams overview

http://www.ready.gov/

http://www.ready.gov/business/index.html Plan to stay in business, Talk to your people, Protect your investment
http://www.ready.gov/index.html Prepare your family, Get a kit, make a plan, stay informed

http://www.redcross.org/

http://www.dola.state.co.us/ Colorado Department of Local Affairs

http://cdpsweb.state.co.us/ Colorado Department of Public Safety

http://www.dhs.gov/dhspublic/ Department of Homeland Security

https://www.llis.dhs.gov/ Lessons learned

CONTACT INFORMATION

Colorado Office of Preparedness and Security
Homeland Security Section
9195 E. Mineral Ave, Suite 234
Centennial, CO 80112
(720) 852-6720
ops@cdps.state.co.us
http://ops.state.co.us/