

Terrorism Protective Measures Resource Guide

Banks and Financial Institutions



Office of Preparedness and Security

December 2006

Forward

The Office of Preparedness and Security (OPS) has developed a series of protective measures for critical infrastructure and key resources (CI/KR). The sector-specific guides compliment the Department of Homeland Security's National Infrastructure Protection Plan (NIPP) and will help CI/KR partners meet the federal security recommendations.

The Department of Homeland Security (DHS) developed the National Infrastructure Protective Plan to establish uniformed federal guidelines for critical infrastructure identification, prioritization and protection. Following the requirements established in Presidential Directive #7 and the Homeland Security Act of 2002, it provides a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect assets from terrorist attacks.

The plan provides a unifying structure built on key initiatives, milestones and metrics required to achieve the nation's critical infrastructure protection mission. It sets national priorities, goals and objectives and will help ensure that government, the economy and public services are sustained in the event of a terrorist attack or natural disaster. It establishes a comprehensive risk management framework, and clearly defined roles and responsibilities for the Department of Homeland Security, federal sector-specific agencies, and other federal, state, local, tribal and private sector security partners.

It is an adaptive architecture, designed to ensure that resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats and minimizing the consequences of terrorist attacks and other incidents.

OPS is committed to the success of the NIPP and to the safety and protection of Colorado. The plan provides a road map for Colorado to sustain the unified effort to protect the assets of Colorado, and ultimately, its citizens. To be successful, this must be a collaborative effort.

The Office of Preparedness and Security, in accordance with DHS, is providing these measures as recommendations and best practices; they are not requirements.

Protective Measures

The purpose of the OPS Terrorism Protective Measures Resources Guides is to provide an overview of the terrorist threats that face our state and the measures we can take to protect ourselves. The primary mission of the Office of Preparedness and Security is to work with Colorado communities to protect our citizens, critical infrastructures and the assets they control. The guides are intended to provide information that can help in determining areas within a facility that are vulnerable to possible terrorist attacks and the ways in which to best protect them.

Protective measures are intended to:

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

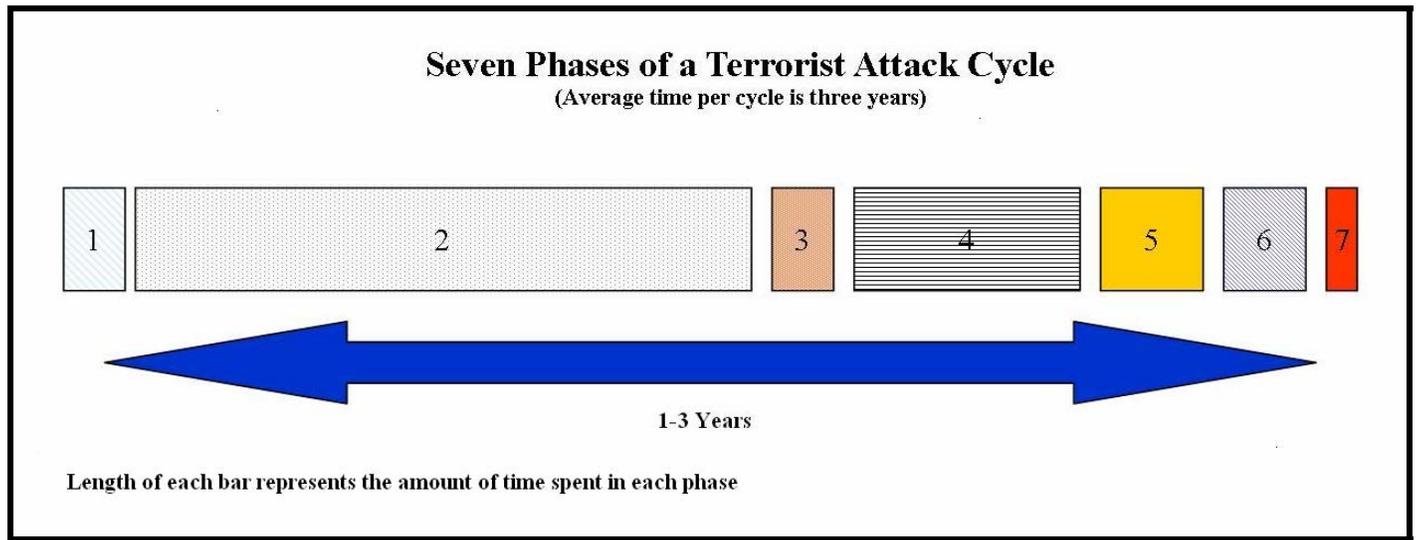
The guides provide an overview of the terrorist attack cycle and terrorist objectives, examples of specific threat categories, available protective measures and their implementation, and a protective measures matrix.

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 customized for the following sector:

Infrastructure: Banks and Financial Institutions



Seven Phases of a Terrorist Attack Cycle



History has shown that terrorist groups tend to target, plan and carry out terrorist attacks using a similar method. The method is referred to as a “terrorist attack cycle.” The cycle has seven phases and the average time frame for a terrorist attack is three years.

This overview of the seven phases begins to explain why and how the following protective measures were developed and to help illustrate why a facility should implement the recommendations.

Phase One: Target Selection

The terrorist begin target selection based on their objectives and capabilities. They select a target with “softness” in mind. They often pick several similar targets with the maximum possible damage and effect caused as the primary consideration.

After the targets have been selected, they begin the fact finding process, collecting site information to determine security weaknesses and vulnerabilities.

Phase Two: Surveillance (Information gathering)

Initial surveillance is conducted on selected soft targets to gather as much information as possible about the targets and narrow the choices. Types of surveillance include foot, vehicle, and technical (camera, video recording). The information is used to determine the opportune time and place for actual attack.

The surveyors are looking for site vulnerabilities by recording and monitoring activity such as types of identification used, existence and location of security cameras, types of locks, location of HVAC systems, gaps in fences or areas that can be accessed without notice and response time of emergency responders.

The surveillance team is usually a stand-alone team, not included in the attack element.

Phase Three: Final Target Selection

Using information obtained through surveillance, terrorists chose their target based on target “softness” and likelihood of overall “mission success.” Key considerations for final target selection include total casualties,

economic damage, fear, damage to confidence in government, possible political targets (politicians) and media attention.

Phase Four: Planning

Planning for the attack includes deciding on the method of attack and obtaining supplies and personnel to carry it out. Based on information and intelligence gathered during the surveillance phase, the method of the attack is decided and the man-power, equipment and training needs to carry out the attack are determined.

Methods of attack include:

- Bombings
- Suicide attacks/bombings
- Arson
- Armed assault
- Hostage-taking
- Other methods – sky-jacking, hi-jacking, kidnapping, assassinations, ambushes, maiming, weapons of mass destruction, and other criminal activities

Supplies required for an attack might include explosives, weapons and ammunition, chemicals, identification, military and law enforcement uniforms, decals and badges, passports and airline tickets.

Phase Five: Final Surveillance

Final surveillance is usually conducted by the individuals carrying out the attack phase, not the initial surveillance team. The terrorists take a last look at the target to insure there have not been any changes in the security posture. They often conduct a “dry run” to test systems and site security.

Phase Six: Deploy Attack Team

The terrorist prepare for the final phase by placing people, equipment and supplies at or near the target.

Phase Seven: Attack

The terrorist carry out their plan.

Implementing protective measures increases security to better deter, defend and devalue a site with regards to a terrorist attack.

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 its surrounding area. 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, protective measures that are specifically orientated towards banks and financial institutions 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 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 anti-terrorism measures.

Protective Measures

The following Exhibits (1-5) are designed to provide information and assistance to facility owners, local law enforcement, and state and local homeland security agencies in making decisions on how to increase security measures on the basis of HSAS alert levels. 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.

Deter	Detect	Devalue	Defend	Protective Measures	Measure Implemented by
-------	--------	---------	--------	---------------------	------------------------

Access Control					
	X	X	X	Ensure that a process is in place for controlling access and egress to the facility	
	X	X	X	Designate points of entry that are monitored to control building access.	
		X		Designate and secure entrances to controlled areas within the facility.	
		X		Secure hazardous materials	
X		X		Provide appropriate signage restricting customers from secure areas.	
	X	X		Control employee identification and access through use of picture badges.	
		X		Control contractor, vendor and temporary personnel identification and access to controlled areas through use of passes or badges.	
		X	X	Review traffic patterns and, where possible, keep cars, buses, and trucks away from facility buildings and areas where crowds congregate.	
		X		Grant access only to authorized personnel when buildings are locked.	
X	X	X		Ensure that the building perimeter is free from trees, branches and telephone poles that may provide access to the building's upper floor or roof.	
		X	X	Restrict other vehicles from access to the bus-loading zones during loading/unloading	
	X	X	X	Formally identify gathering areas in locations that have nature surveillance and access control or are out of view of the would-be offender. Then make informal gathering areas off limits and the subject to automatic scrutiny.	
		X		Ensure that low canopies or awnings have protective parapets to deter their use for climbing onto roofs.	
		X	X	Ensure that the mechanical, electrical, and other equipment on the ground is surrounded by a protective enclosure.	
		X		Design and locate roof access ladders to prevent unauthorized access to the roof.	
		X	X	Close off areas of the facility not in use after hours.	
		X		Protect high-risk areas, such as offices, cafeteria, computer rooms by use of high-security locks and an alarm system.	
		X	X	Maintain physical security on mechanical rooms to prevent the direct introduction of hazardous materials into air-distribution ducts. Lock and control access to all mechanical rooms containing heating, ventilation and air-conditioning equipment.	
X	X	X	X	Identify, secure, and control access to all utility services to the facility. Limit and control access to all facility crawl spaces, utility tunnels, and other means of under-building access to prevent the planting of explosives.	
		X		Define controlled areas requiring security (e.g., buildings, housing areas, laboratories, control rooms and maintenance areas).	
Barriers					
X			X	Provide Adequate perimeter fencing or walls around grounds.	
		X	X	Place physical barriers between buildings and roadways or other drivable areas.	
		X	X	Avoid long, straight layouts for parking lots, especially those used by customers or, if not possible, install speed bumps to reduce vehicle speeds.	
		X	X	If fire lanes around the building are required, close them off from maintenance and other traffic with "breakaway" bollards and, preferably, with a hardened surface with grass sown above.	
		X	X	Ensure that deep recesses in the buildings with wings are fenced and well lit.	
		X	X	Ensure that all exterior doors have non-removable hinge pins, have no exterior hardware or protective plates covering locks and/or have plates covering gaps between the door and jam.	
X	X	X	X	Review landscaping and ensure that buildings are not obscured by overgrowth of bushes or shrubs where contraband can be placed or persons can hide.	
X			X	Apply protective coating on windows in facilities that face traffic.	
X		X		Install secure locks for all external and internal doors and windows.	
X		X		Install window and external door protections with quick-release capability.	

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
---------	--------	-------	--------	---------------------	------------------------

				Monitoring and Surveillance	
	X	X		Provide adequate lighting on grounds and in the buildings. Ensure that entrances and other points of possible intrusions are well lit and that the building has adequate outside lighting to enhance night safety.	
	X			Provide intrusion-detection systems at all controlled areas.	
	X	X		Provide video surveillance systems on grounds and in buildings.	
	X	X	X	Maintain visual surveillance of parking lots, ball fields and other exterior areas or monitor by remote security cameras from the security office or some other central location.	
	X	X	X	Ensure that remote camera locations provide maximum coverage of the grounds and that view angles of security cameras are free and unobstructed by building elements or trees.	
	X	X		Arrange for law enforcement, security or other staff members to patrol parking areas during hours.	
	X	X		Ensure that security patrols have appropriate access to buildings and the grounds after hours.	
	X	X		Ensure that the parking lot lighting provides uniform coverage that supports camera surveillance.	
	X	X		Ensure that lighting fixtures and remote cameras are protected with vandalism-proof covers or are located high enough to prevent vandalism.	
	X	X		Assign staff members or security personnel to monitor or have a security camera monitor the main entrance lobby.	
				Communications	
		X	X	Maintain instantaneous communication capability with administrative and security elements.	
		X	X	Establish close ties with local and/or state law enforcement agencies. Develop liaison with local law enforcement and emergency response teams to enhance information exchange, clarify emergency response, track threat conditions and support investigations.	
			X	Develop communication process with general public regarding situations and incidents. Have a plan for communicating information to customers and for quelling rumors. Cultivate relationships with the media ahead of time and identify a public information officer to communicate with the media and the community during a crisis.	
X		X	X	Establish a facility-wide telephone system.	
	X	X	X	Ensure a process is established for communicating with customers and staff during a crisis.	
X		X		Inspect equipment to ensure operation.	
X	X	X	X	Work with law enforcement officials and emergency preparedness agencies on a strategy for sharing key parts of the facility crisis plans.	
	X		X	Arrange for alarm systems to be remotely monitored by local law enforcement or emergency response agencies.	
				Inspection	
		X	X	Check and inspect emergency building systems, fire alarms, emergency generators and exit lights.	
	X	X	X	Check outdoor air intakes of HVAC systems to ensure that they are protected.	
	X	X	X	Locate outdoor air intakes of HVAC systems in or on a building wall at least at the second story level, preferably higher. For rooftop or ground level intakes that can not be modified, establish a security zone to limit access.	
		X		Define controlled areas requiring security, including buildings, control rooms, maintenance areas, receiving areas, shipping areas, pipelines and valves and storage tanks, if present.	
	X	X	X	Inspect facility lighting protection systems and ensure all wires and cables are connected.	
				Security Force	
X	X	X	X	Maintain an adequately staffed and equipped security force. Train and prepare security force to recognize potentially dangerous situations at and around the facility.	
X	X	X	X	Conduct regular patrols of grounds, buildings and facilities.	
	X		X	Conduct drills and exercises for security force.	
	X		X	Train and prepare security force to recognize potentially dangerous situations on and around facility.	
	X	X		Assign security officers as liaisons with international groups.	

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.

Deter	Detect	Devalue	Defend	Protective Measures	Measure Implemented by
Cyber Security					
	X	X	X	Develop secure information technology network.	
		X	X	Control access to information technology systems (on-site, remote access).	
			X	Maintain backup information technology systems.	
	X	X	X	Locate mission-critical system facilities in a secure location that is locked and restricted to authorized personnel only.	
	X	X	X	Physically secure personal computers in an area that is inaccessible to unauthorized users.	
	X	X	X	Check the credentials of external contractors working on the information.	
X	X	X	X	Ensure that operating systems are updated with current security patches.	
X	X	X	X	Use and regularly update anti-virus software.	
	X	X	X	Control access to critical computer hardware, wiring, displays and networks by rules of least privilege.	
		X	X	Document system configurations (i.e., hardware, wiring, displays and networks) of critical systems. Govern installations and changes to those physical configurations by a formal change management process.	
	X	X	X	Implement a system of monitoring and auditing physical access to critical computer hardware, wiring, displays, and networks (e.g., badges, cameras, access logs).	
Security Program					
	X		X	Invite local and state law enforcement officers to the facility to help them become familiar with the institution, its leadership and the complexity of its operations.	
	X		X	Raise awareness among law enforcement officers and facility officials by conducting exercises relating to emergency and crisis management plans.	
			X	Become involved in regional "Homeland Security" planning.	
X	X	X	X	Conduct threat analysis, vulnerability assessment, consequence analysis and risk assessment.	
X	X	X	X	Establish "Threat Assessment Teams" and develop checklists for each level of threat identified by the Department of Homeland Security.	
X	X	X	X	Develop comprehensive written plans, policies, and procedures.	
	X	X		Conduct employee background screening.	
X	X	X	X	Refine and exercise preplanned protective measures, as appropriate.	
X		X		Restrict access to facility building data. Control information on building operations (including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics and emergency operations procedures).	
X	X	X	X	Ensure that all facilities are assessed for vulnerabilities to emergencies and terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities.	
	X	X	X	Disseminate written instructions for use by personnel in emergency situations.	
X		X	X	Establish a safe area or areas within the facility for assembly and shelter during emergencies.	
	X	X	X	Develop a security awareness program for visitors and employees	
	X	X	X	Conduct awareness training relating to the facility that includes awareness of signs of terrorism for employees and visitors	
		X	X	Work with businesses and factories near the facility to ensure that the facilities crisis plan is coordinated with their crisis plans.	
X	X	X	X	Update individual facility crisis plans yearly to include evacuation and shelter-in-place plans.	
	X	X	X	Provide a copy of the Red Cross brochure "Terrorism: Preparing for the Unexpected" (http://www.redcross.org/service/disaster/keepsafe/terrorism.pdf) staff.	
	X	X	X	Coordinate emergency/security plans with local, state and federal plans.	
Incident Response					
			X	Develop a unified command plan with local government and law enforcement agencies and conduct an annual review of the plan.	
			X	Establish a management team responsible for directing the development and implementation of a facility-wide emergency operations plan.	
			X	Maintain an adequately staffed, equipped, and trained emergency response team.	
			X	Conduct drills and exercises for the emergency response team on a regular basis.	

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	Establish an Emergency Operations Center.	
			X	Conduct fire and safety drills for the entire campus community.	
X	X	X	X	Conduct an assessment of each building. Identify factors that put the building, visitors and staff at a greater risk, such as proximity to rail tracks that regularly transport hazardous material or propane gas tanks or facilities that produce toxic materials and develop a plan to reduce the risk.	
			X	Have site plans for each facility readily available and ensure they are shared with first responders and agencies responsible for emergency preparedness.	
		X	X	Assign responsibility to specific staff members for turning off the gas, electricity, water and alarm in case of an emergency and inform all staff of the assignments.	
			X	Ensure that there are multiple evacuation routes and rallying points. First or second evacuation site options may be blocked or unavailable at the time of the crisis.	
		X	X	Inspect equipment to ensure that it is in good working conditions.	
			X	Develop a command structure for responding to a crisis. Develop, review, and approve the roles and responsibilities for staff, law enforcement and fire officials and the first responders in responding to different types of crisis.	
			X	Identify and approve a team of credentialed mental health workers to provide mental health services to a staff after a crisis.	
			X	Ensure that staff (including security and law enforcement personnel) are trained in implementing the facilities crisis management plan.	
			X	Ensure that the facility security officers receive in-service training related to their responsibilities and in compliance with the facilities policies. Ensure that staff members have been trained in how to respond appropriately to suspicious materials, packages, items and situations.	
			X	Obtain and maintain emergency supplies and equipment.	
			X	Create crisis and evacuation kits and place them at strategic locations inside and outside of the facility.	
				Personnel Protection	
		X	X	Provide safety and security briefings to all staff.	
X	X	X	X	Ensure personnel receive proper training on personal protective measures.	
X		X		Establish restrictions on loitering in parking lots, hallways, bathrooms and other areas.	
				Infrastructure Interdependencies	
			X	Provide adequate utility services.	
			X	Provide backup for critical utility services.	
		X	X	Provide adequate security for utility services.	
	X	X	X	Secure and enclose dumpsters to prevent persons from climbing inside, hiding, or concealing weapons or hazardous materials. Construct 8-ft-high screen walls around three sides to prevent climbing. Ensure that the gate side is lockable and provides visual access to the inside of the enclosure.	
			X	Provide an emergency power source for critical systems such as exit signs, fire alarm systems, illuminate exit paths, emergency voice/alarm communication systems, and elevator car lighting. Provide stand-by power for smoke management systems, fire pumps, elevators and emergency power loads.	
	X		X	Connect ductwork smoke detectors into the fire alarm system and design to automatically shut down air handling units.	

Exhibit 2 Protective Measures Implemented at HSAS Threat Level blue

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	X	Control entrance to sensitive areas through manned security checkpoints.	
		X		Secure building, rooms, and storage areas not in normal use.	
	X	X		Reinforce that identification badges be displayed at all times.	
		X		Ensure that only essential vehicles are given access to controlled areas.	
				Barriers	
		X		Review security hardware on doors, locks and windows.	
		X		Check fences and lighting.	
			X	Check HVAC shutoff and intake controls.	
				Monitoring and Surveillance	
	X			Check operation of closed circuit television.	
				Communications	
		X	X	Check facility communications systems, including security radios. Have a supply of batteries ready.	
	X	X	X	Ensure that radio/phone contact with local law enforcement works.	
	X			Ensure that alarm systems work.	
		X	X	Check communications with designated response or command locations.	
X	X	X	X	Provide the public with information so people can act appropriately.	
	X		X	Check security radios and ensure batteries are readily available.	
				Inspection	
	X	X		Conduct security a spot checks of individuals entering controlled area.	
	X	X		Conduct security spot checks of vehicles entering controlled areas.	
		X	X	Check and inspect emergency building systems, fire alarms, emergency generators and exit lights.	
				Security Force	
	X	X	X	Review existing countermeasures and operational procedures to ensure the adequacy of guard allocation and access control procedures.	
	X	X	X	Conduct comprehensive patrols of the entire facility, including out buildings and the grounds.	
				Cyber Security	
	X			Increase monitoring of all external network connections.	
			X	Ensure coordination with supporting telecommunication restoration priorities and plans.	
			X	Increase the frequency of critical backup plans.	
				Security Program	
	X	X		Maintain vigilance on changes in vendor personnel who have site access.	
			X	Conduct tabletop emergency response exercises.	
				Incident Response	
		X	X	Put key personnel on call who can implement security plans and seal off areas.	
			X	Review contingency plans, evacuation/relocation plans and emergency response procedures/manuals.	
			X	Check plans for implementation to next threat level.	
			X	Conduct pre-incident liaison and planning with federal or other weapons of mass destruction response organizations, as appropriate.	
				Personnel Protection	
	X	X		Advise personnel on rising threat level.	
	X	X		Reinforce personal security awareness.	
		X	X	Consider enhanced security measures for high-profile administrators and faculty members.	
				Infrastructure Interdependencies	
		X		Check barriers around utility supply points e.g., fences, locks).	

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	X	X	Establish a single point of access to each building/facility and institute 100 % identification checks.	
	X	X	X	Increase administrative inspections of persons and their possessions entering critical facilities.	
		X		Limit access to critical facilities within/outside the facility building(s) to an absolute minimum.	
		X		Escort all visitors and non-employees within the critical facilities at all times.	
		X		Prevent vehicles from parking within 25 meters of buildings and other structures.	
		X		Consider centralizing parking.	
		X		Require that a host be contacted to authorize visitor entry to the critical facilities.	
		X		Limit the number of vehicle entry points into facility.	
	X	X		To deter tampering by outside maintenance personnel, ensure that a staff member visually inspects their work before final acceptance of the service. Alternatively, ensure the reliability of prescreened service personnel from a trusted contractor.	
		X	X	Physically isolate lobbies, mailrooms, loading areas, and other entry and storage areas from the rest of the building.	
				Barriers	
		X	X	Assess the adequacy of physical barriers outside buildings and the proximity of parking.	
		X		Consider retrofitting existing streets with barriers, bollards, swing gates or other measures to force vehicles to travel in a serpentine path.	
		X		For high risk buildings, consider providing additional protection by creating a clear zone immediately adjacent to the structure that is free of all visual obstructions or landscaping.	
		X	X	Cover HVAC intakes with screens so that objects cannot be tossed into them or into air wells from the ground.	
		X	X	When possible, designate an entry point to the facility for commercial, service and delivery vehicles, preferably away from key facility areas and functions.	
				Monitoring and Surveillance	
	X	X		Assess the adequacy of video monitoring. Install additional CCTV cameras in areas where needed.	
	X	X		At the beginning and end of each day, inspect interior/exterior of building and storage areas in regular use.	
	X	X		Increase building spot checks.	
	X	X		Provide CCTV video feed to local law enforcement.	
	X			Check HVAC filtration, any detectors and monitors and alarm systems.	
	X	X	X	Increase surveillance of critical locations.	
				Communications	
		X	X	Ensure the adequacy of emergency alert and communication systems for staff and visitors.	
	X	X	X	Enhance interface with local law enforcement, safety and related emergency groups.	
	X	X	X	Conduct additional briefings for administrative personnel, faculty and students.	
			X	Provide backup power source for communication equipment.	
	X	X	X	Test alternative communication service (e.g., radio or cellular telephones) to ensure that communications function in case of an incident.	
	X	X		Reemphasize to staff and visitors the need to report suspicious activity to the proper authorities.	
				Inspection	
	X	X		Increase physical checks of critical facilities during periods of increased alert.	
	X	X		Randomly inspect visitors' briefcases, backpacks and other packages.	
	X	X		Increase frequency of personnel spot checks and vehicle spot checks.	
	X			Raise awareness regarding delivery of suspect mail packages.	
	X			Enhance mail inspection procedures.	
				Security Force	
	X	X	X	Consider guard reinforcement and ensure that guards are adequately trained in procedures.	
	X	X	X	Expand roving/motorized patrols to outer perimeter.	
	X	X		Require security guards to visually inspect the interior and exterior of all vehicles entering the main gate. Do a brief visual inspection by walking around the vehicle and looking inside the cab and cargo area. No undercarriage inspection.	

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	X	Enhance mail inspection procedures.	
				Cyber Security	
X		X		Delete part or all of the facility information from public accessed Web site.	
	X			Increase frequency of cyber system monitoring.	
				Security Program	
X	X	X	X	Assess if preplanned protective measures need refinement.	
X	X	X	X	Implement, as appropriate, contingency and emergency response plans.	
				Incident Response	
			X	Ensure that all personnel responsible for countermeasures are on call.	
			X	Review lock down/shutdown plans.	
			X	Ensure operability of Emergency Operations Center.	
			X	Consider having shelter-in-place rooms or areas in building, where people can stay in the event of an outdoor toxic agent release.	
				Personnel Protection	
	X	X		Update personnel on rising threat.	
		X	X	Implement additional security measures for high-profile administrators and faculty.	
				Infrastructure Interdependencies	
		X	X	Add barriers to utility supply points.	
X	X	X	X	Increase patrols at utility supply points.	

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		Establish security checkpoints to keep adversaries distant from the building. Consider closing roads.	
		X		Strictly enforce access controls.	
		X		Restrict access to facility to essential operational purposes only.	
		X		Enforce centralized parking away from buildings and arrange security for those vehicles	
		X		Consider restricting parking to locations outside the grounds.	
		X		Restrict deliveries to daytime hours only.	
		X		Cancel or delay non-vital contractor work.	
		X		Require vendors and contractors to be on a pre-approval list.	
		X		Restrict threatened facility access to essential personnel only.	
		X		Require visitors to be escorted at all times in sensitive areas.	
				Barriers	
		X	X	Secure and regularly inspect all buildings, rooms and storage areas.	
		X	X	Erect barriers and obstacles to control vehicle flow through the facility.	
		X	X	Erect Jersey barriers at buildings and critical facilities.	
		X	X	Use vehicles as temporary physical barriers by placing them in front of critical facilities or across access roads.	
		X	X	Use high curbs, low berms, shallow ditches, trees, shrubs and other physical separations to keep potential stationary bombs at a distance.	
		X	X	Do not allow vehicles to park next to perimeter walls of the secured area. Consider using bollards or other devices to keep vehicles away.	
		X		Design (if they are required) traffic-calming strategies and barriers Road alignment, retractable bollards, swing gates, or speed bumps) to control vehicle speed and slow incoming vehicles before they reach the gate so that entry personnel have adequate time to respond to unauthorized activities.	
		X	X	Provide passive vehicle barriers to keep potential stationary vehicle bombs at a distance from the building.	
				Monitoring and Surveillance	
	X	X		Install additional temporary lighting at critical assets and key locations throughout facility.	
	X	X		Increase lighting in buffer zones.	
				Communications	
	X	X	X	Provide daily security and awareness briefings to staff.	
X				Prepare to handle inquires from anxious visitors and media.	
				Inspection	
	X	X		Check/screen all deliveries.	
	X	X		Increase frequency of random inspections of visitors' briefcases, backpacks and other packages.	
	X	X		Search all vehicles and contents before they are allowed to enter the campus grounds.	
	X	X		Provide inspection areas that are not visible to the public. Place appropriate landscape planting to accomplish screening.	
	X	X		Provide pull-over lanes at facility grounds entry area to check suspect vehicles. Also, provide a visitor / site personnel inspection area to inspect vehicles prior to allowing them access to the facility grounds.	
				Security Force	
	X	X	X	Increase number of security guards and patrol activities.	
		X	X	Consider deployment of law enforcement personnel and instruct guards on procedural implications.	
		X	X	Provide additional weapons and equipment to security force.	

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		Use an explosive-detecting K-9 unit.	
				Cyber Security	
		X		Reduce the number of people authorized to access computer systems.	
		X		Disable access to the internet and other portals that might allow unauthorized access.	
		X	X	Implement more frequent back-up procedures.	
				Security Program	
		X		Evaluate the risk of public events and take the necessary precautions.	
X	X	X	X	Prepare to execute contingency plans.	
X				Consider canceling outside activities, sporting events and high profile activities.	
		X		Prohibit vehicles from leaving site without pass.	
				Incident Response	
			X	Ensure that all personnel responsible for implementing countermeasures are immediately available.	
			X	Add firefighting and emergency medical personnel to shifts.	
			X	Activate the Emergency Operations Center.	
				Personnel Protection	
	X	X		Update personnel on escalating threat level.	
			X	Verify shelter-in-place procedures and equipment.	
			X	Ensure that the best available filtration is being used for the existing HVAC configuration.	
				Infrastructure Interdependencies	
		X	X	Add barriers to critical utility supply points.	
		X	X	Where possible, provide additional backup utility supplies (e.g., backup generator).	
		X	X	Provide additional monitoring of utility supply points.	

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		Coordinate with local authorities regarding closing of public roads and facilities	
		X		Do not permit visitors.	
	X	X		Do not permit nonessential vehicles. Thoroughly search all vehicles entering facility, including undercarriage.	
X		X	X	Prepare to close facility.	
X		X	X	Further limit parking near critical buildings to increase stand-off distance.	
		X		Monitor, redirect or constrain transportation systems.	
Barriers					
		X		Deploy temporary barriers at all key locations not already protected.	
			X	Move objects that could become projectiles 25 meters away from buildings.	
		X		Provide a vehicle crash resistant system in the form of a low wall or earth berm, if warranted.	
		X		Install traffic obstacles near entry control points to slow down traffic.	
		X		Offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed.	
		X		Position gates and perimeter boundary fences outside the blast vulnerability envelope, when possible.	
Monitoring and Surveillance					
	X	X		Make frequent checks of all exterior areas of the facility, including parking.	
	X	X		Leave lighting on 24/7	
Communications					
			X	Test communications and notification procedures.	
			X	Advise site management / personnel of potential need to implement evacuation/relocation plan.	
			X	Conduct daily briefings with local law enforcement on threat condition.	
Inspection					
	X	X		Search all persons before they enter the facility.	
	X	X		Search all vehicles and contents before they enter grounds.	
	X			Process mail off-site.	
		X	X	Pick up and store all loose items, such as trash cans, benches, newspaper racks, cigarette urns, traffic cones, barriers, free standing signs, recyclable containers or any items not permanently attached to the building.	
Security Force					
	X	X	X	Patrol entire facility and grounds continually.	
		X	X	Augment security guards with law enforcement/military personnel where feasible. Ensure that law enforcement officers are on the site 24 hours as available.	
		X	X	Consider the use of armed guards.	
		X	X	Deploy mobile command post on grounds.	
		X	X	Increase or re-direct personnel to address critical emergency needs.	
Cyber Security					
		X	X	Restrict computer access to essential personnel only.	
	X	X	X	Increase security levels to maximum.	
Security Program					
	X	X		Verify identities of all personnel working in critical areas.	
X				Coordinate with local and state officials to assess threat level to consider openings and closings.	
			X	Activate command and support centers if appropriate.	
	X	X		As feasible, have employees work in pairs.	
Incident Response					
			X	Check all available emergency equipment.	
			X	Add firefighter and emergency medical personnel to shifts.	
			X	Assign emergency response personnel.	
	X	X	X	Pre-position and mobilize specially trained teams or resources.	
	X	X	X	Assign staff members to local government Emergency Operations Center for 24/7	
		X	X	Place transportation resources on standby status.	

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
		X	X	Inventory and refuel transportation equipment.	
				Personnel Protection	
	X	X		Update personnel on escalating threat.	
			X	Establish positive control on building air intakes. Prevent all unfiltered air from reaching manned spaces.	
			X	Ensure that security force and emergency responders have breathing apparatus, if appropriate, and are prepared to evacuate or shelter-in-place.	
				Infrastructure Interdependencies	
X	X	X	X	Provide continuous guard at utility supply points.	

Assessment Service

The Office of Preparedness and Security maintains a specialized team to provide onsite vulnerability assessments. With these assessments, a trained team will come to your facility and assess it for common vulnerabilities based on state and federal guidelines. 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 protected by Colorado state law. The results are provided only to the site.

Please contact OPS at 720-852-6720 or email Sgt. Leonard Dittman at leonard.dittman@cdps.state.co.us to obtain more information on this service and to schedule an assessment.

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/>

REFERENCES

Department of Homeland Security, Protective Security Division
"Protective Measures Infrastructures"
Information Guide
March 11, 2005

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](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

<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, and stay informed

Colorado Office of Preparedness and Security Homeland Security Section

<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.ilis.dhs.gov/> Lessons learned

Pantera, M.J., III, et al., "Best Practices for Game Day Security at Athletic and Sport Venues," The Sports Journal: <http://www.thesportjournal.org/2003Journal/Vo16-No4/security.asp>

FEMA, Appendix D, "Cyber-terrorism," in FEMA Toolkit: http://www.fema.gov/txt/onp/toolkit_app_d.txt

Pantera, M.J., III, NCAA News

Planning Is Key to Locking Down Security

<http://www.ncaa.org/news/2003/20030818/editorial/4017n30.html>