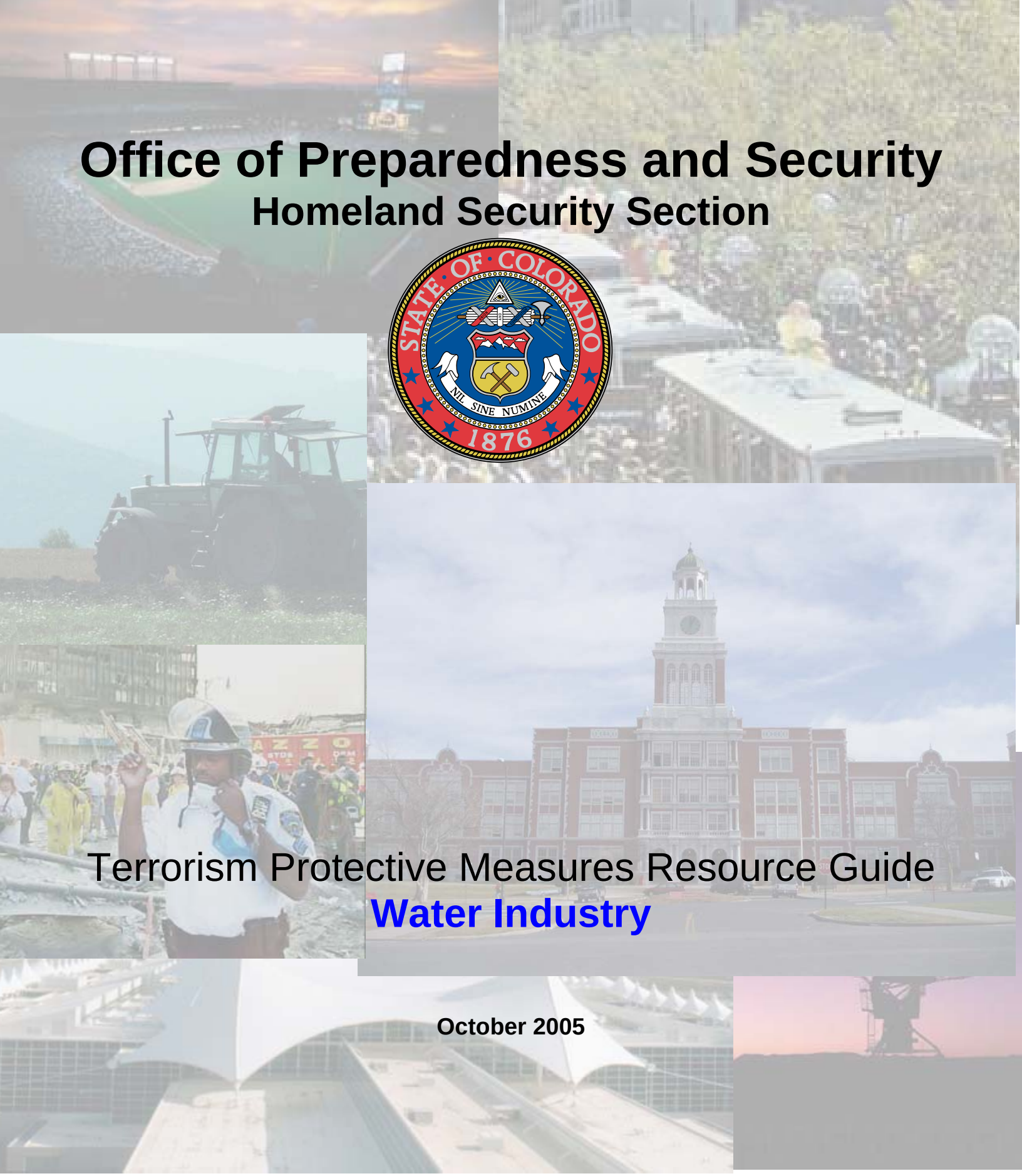
Office of Preparedness and Security
Homeland Security Section



Terrorism Protective Measures Resource Guide
Water Industry

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 Colorado 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, 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 (OPS) also maintains a specialized team (Team Rubicon) to provide 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 are exempt from Colorado's Open Records Law.

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.

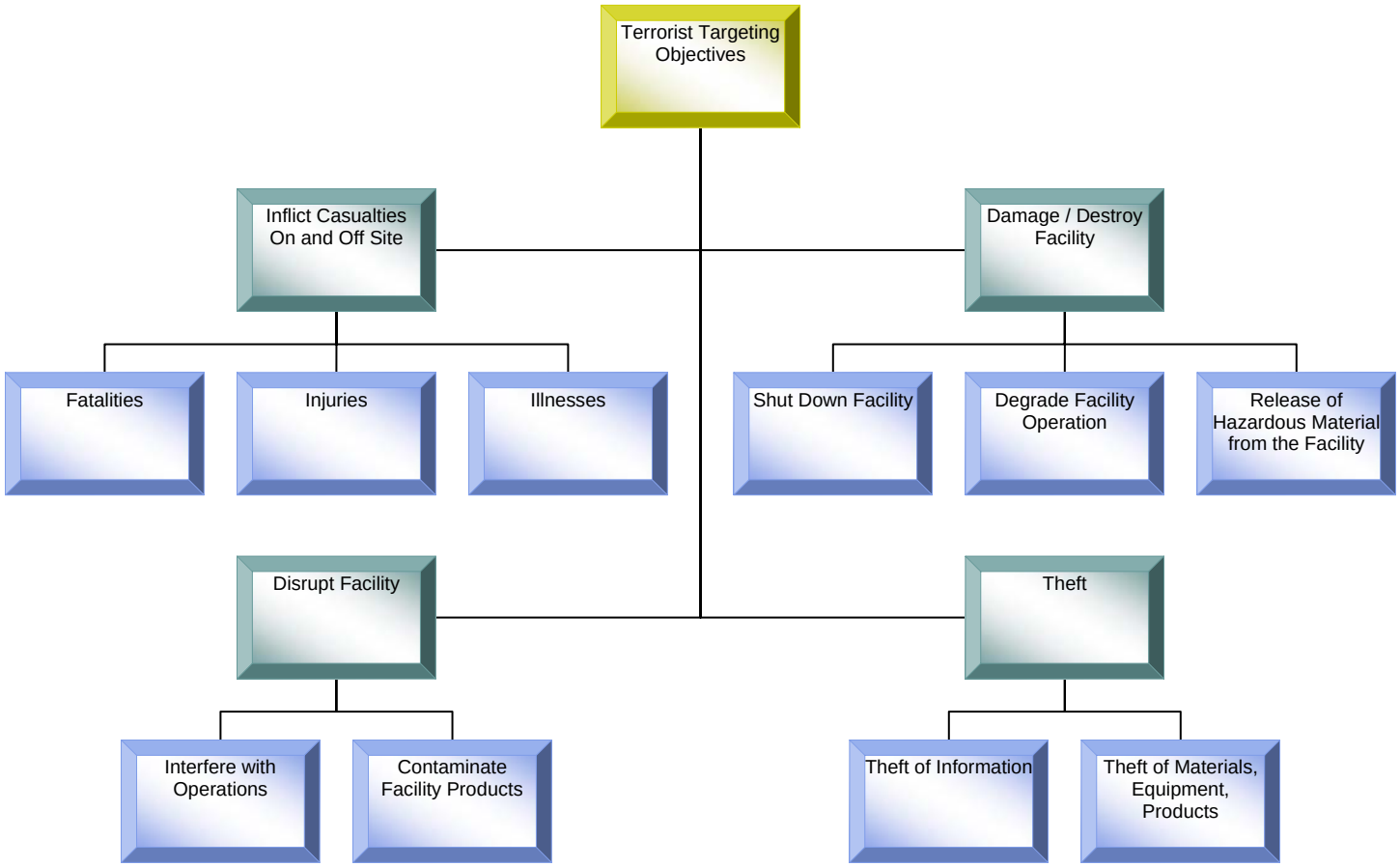
There are thirteen critical infrastructure sectors and four key resource segments. While a number of protective measures can be implemented for any of the thirteen critical infrastructure sectors, this guide is customized with protective measures customized for the following sector:

Infrastructure: Water Industry

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 water.

Figure 1



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 have 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 Water industry 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, Earth banks and berms (e.g., for blast protection)
	Fences (e.g., barbed wire, chain link)
	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
Low Risk of Terrorist Attack

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		Require visitors to wear badges and sign in/out of the facility.	
		X		Escort all visitors at all times.	
		X		Prosecute intruders, trespassers and those detained for tampering.	
		X		Review requests for tours and identify protocols for managing the tours.	
		X		Ensure that all employees wear identification badges while in the facility.	
		X		Implement controls for construction activities at critical sites and in critical areas.	
		X	X	Fence and lock the facility and vulnerable areas. (e.g., wellheads, hydrants, manholes and storage tanks).	
		X	X	Lock all entry gates and doors and set alarms to alert illegal entry. Do not leave keys in equipment or vehicles at any time.	
		X	X	Secure vehicles and equipment.	
		X	X	Lock monitoring wells to prevent vandals or terrorists from pouring contaminants directly into source water.	
X		X	X	Prevent pouring or siphoning of contaminants through vent pipes by moving the vent pipes inside the pump house or treatment plants or if that isn't possible, fence or screen them.	
				Barriers	
X		X		Provide adequate perimeter fencing at appropriate points.	
		X		Maintain clear zones at fence lines. (e.g., keep shrubs away from fences).	
				Monitoring and Surveillance	
	X			Monitor water quality at the source water, leaving the plant and in distribution and storage systems. Establish baseline conditions. Review operational and analytical data to detect unusual variations.	
	X			Monitor influent, process unit and effluent water quality in accordance with established water reclamation plant operation and monitoring programs. Establish baseline results. Review operational and analytical data to detect unusual variations.	
	X			Maintain surveillance of commercial/industrial/government dischargers. Review operational and analytical data to detect unusual variations (e.g., changes in production, chemical and waste accumulation/storage).	
	X			Follow up on customer complaints concerning water quality and/or suspicious behavior at the facilities.	
	X			Implement best-management practices for optimizing drinking water treatment.	
	X	X		Install good light around the pump house, treatment facility and the parking lot.	
	X	X		Maintain vigilance and be alert to suspicious activity. Report suspicious activity to authorities.	
				Communications	
		X	X	Confirm communication protocol with public health officials concerning potential water-borne illnesses.	
			X	Identify sensitive populations within the service areas (e.g., hospitals, nursing homes, daycare centers, schools) for notification, as appropriate, in the event of a specific threat against the utility.	
		X	X	Contact local police and ask them to add facility to their routine patrol.	
				Inspection	
	X	X		Check all chemical deliveries for driver verification and verification of load.	
X		X		Inventory spare parts and on hand chemicals. Confirm they are sufficient.	
	X	X		Routinely inspect building within the facility for suspicious packages and evidence of unauthorized entry.	
X		X		Conduct routine inventories of emergency supplies and medical kits.	
	X	X		Test security alarms and systems for reliability.	
				Security Force	
X	X	X	X	As appropriate, employ security force. Have security be visible as much as possible.	

Exhibit 1 Protective Measures Implemented at HSAS Threat Level Green
Low Risk of Terrorist Attack

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
				Cyber Security	
X			X	Back up critical files, such as plans and drawings, as-builts, sampling results, billing and other critical information.	
				Security Program	
	X	X	X	Monitor requests for potentially sensitive information.	
X	X	X	X	Prepare vulnerability assessments and revise to incorporate changes made (e.g., assets, added/replaced or new countermeasures implemented).	
	X	X		Conduct appropriate background investigations on staff, contractors, operators and others who have access to the facility.	
X		X	X	Identify existing and alternative water supplies and maximize the use of back-flow prevention devices and interconnections.	
		X	X	Review commercial/industrial/government discharger spill prevention, control and countermeasures plan for adequacy and address identified deficiencies.	
X		X	X	Maintain disinfectant residuals as required by regulations.	
				Incident Response	
			X	Prepare or update an emergency response plan. Make sure all employees help to create it and receive training on the plan.	
			X	Post emergency evacuation plans in accessible, but secure, location near entrance for immediate access by law enforcement, fire response, and other first responders.	
			X	Post updated emergency 24 hour phone numbers in highly visible areas (e.g., pump house door, vehicles, and offices) and give them the to key personnel and local response officers.	
				Personnel Protection	
		X	X	Train staff in safety procedures, such as handling hazardous materials and maintaining and using self-contained breathing apparatus.	
			X	Ensure that employees understand appropriate emergency notification procedures.	
			X	Provide emergency preparedness information and training to employees.	
			X	Conduct training, seminars, workshops and exercises using the emergency response plans.	
				Infrastructure Interdependencies	
X			X	Review infrastructure sources (e.g., electric power, telecommunications) and provide backup capability as appropriate.	

Exhibit 2 Protective Measures Implemented at HSAS Threat Level yellow General Risk of Terrorist Attack

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		Control access to mission-critical facilities.	
		X		Ensure that everyone on site is appropriately badged.	
		X	X	Implement controls at critical facilitates undergoing major construction to ensure that contractor personnel do not have access to the entire facility.	
		X		Secure buildings, rooms and storage areas that are not used regularly.	
		X		Maintain a list of secured areas or facilities and monitor activities.	
				Barriers	
		X		Review operational readiness of all barriers.	
				Monitoring and Surveillance	
	X			Report to security any suspicious personnel, particularly those carrying suitcases or other containers or those observing, photographing or asking unusual questions about the treatment facilities, pumping or pipeline operations, or security operations.	
	X			Report to security any unidentified vehicles parked or operated in a suspicious manner or in the vicinity of critical facilities, appurtenances or right-of-ways.	
				Communications	
		X	X	Reaffirm communication and coordination protocols (embedded in the utility's emergency response plan) with local authorities, such as police and fire departments, HAZMAT teams, hospitals and other first responders.	
			X	Prepare draft press releases, public notices, and other communications for a variety of incidents. Route through appropriate channels of review to ensure that pieces are clear and consistent.	
	X			Test security alarms and systems for reliability.	
				Inspection	
	X	X		Instruct employees to "walk the facility" and make general inspections of the grounds, buildings, rooms and storage areas not in regular use and be familiar with the external perimeter. The employees are to check for suspicious activity or packages as part of normal daily operations.	
				Security Force	
	X	X	X	Deploy a security officer at mission-critical sites. The security operations staff will inform contract security personnel of the general threat level and periodically update personnel as the situation changes.	
				Cyber Security	
	X			Increase monitoring of all external network connections.	
			X	Ensure coordination with the supporting telecommunication restoration priorities and plans.	
X			X	Increase the frequency of mission-critical data backup.	
				Security Program	
	X	X	X	Request all employees monitor requests for potentially sensitive information (e.g., scrutinize public information requests, delete items from web site).	
				Incident Response	
			X	Prepare and/or revise emergency response plans and associated communication protocols. Include appropriate local officials concerned with law enforcement, emergency response and public health.	
				Personnel Protection	
			X	Advise personnel of rising threat.	
			X	Reinforce personal security awareness.	
			X	Post employee reminders regularly about events that constitute security violations and ensure that employees understand notification protocol in the event of a security breach.	
				Infrastructure Interdependencies	
			X	Inspect and repair or enhance as necessary all supporting infrastructure facilities (e.g., electric power, telecommunications).	

Exhibit 3 Protective Measures Implemented at HSAS Threat Level yellow Significant Risk of Terrorist Attack

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 all facility tour requests before approving. If a tour is allowed, implement security measure to include a list of names prior to the tour, request identification of each attendee prior to the tour, prohibit backpacks/duffle bags, cameras and enforce parking restrictions.	
		X		Verify the identity of all personnel entering the facility. Mandate visible use of identification badges. Randomly check identification badges and cards of those on the premises.	
		X		Consider steps needed to control access to all areas under the jurisdiction of the water utility.	
		X		At the discretion of the facility manager or security director, remove all vehicles and objects (e.g., trash containers) located near mission-critical areas in the facility.	
		X	X	Maximize physical control of all equipment and ensure that vehicles that are not in use are inoperable (e.g., lock steering wheels, secure keys, chain and padlock front-end loaders).	
				Barriers	
		X		Install a no-climb fence around the perimeter.	
		X		Place empty chemical containers in front of full containers (e.g., empty chlorine tanks should be placed in front of those that are full).	
				Monitoring and Surveillance	
	X			Increase the frequency and extent of monitoring activities and review the results against the baseline.	
	X			Increase the review of operational and analytical data (including customer complaints) with an eye toward detecting unusual variability (as an indicator of unexpected changes in the product). Variations due to normal or routine operational variability should be considered first.	
	X			Increase surveillance activities with regard to critical commercial/industrial/government dischargers (e.g., facilities with substantial chemical storage) and in remote/isolated reaches of the service areas where illicit dumping might occur.	
	X			Increase surveillance activities in source and finished water areas.	
	X			Continuously monitor and record CCTV.	
	X	X		Install perimeter lighting to facilitate surveillance.	
				Communications	
		X	X	Contact neighboring water utilities to review coordinated response plans and mutual aid during emergencies	
			X	Review draft communications on potential incidents, brief media relations personnel of potential for press contact and/or issuance of release.	
		X	X	Reconfirm that county and state health officials are on elevated alert and will inform water utilities of any potential waterborne illnesses.	
		X	X	Review and update list of sensitive populations within the service area, such as hospitals, schools, etc…, for notification, as appropriate, in the event of a specific threat against the utility.	
				Inspection	
	X	X		Perform a daily inspection of the interior and exterior of buildings in regular use for suspicious activity or packages, signs of tampering or indications of unauthorized entry. Ensure that vacant areas are secured.	
X		X		Review whether critical replacement parts are available and accessible.	
	X	X		Inventory chemical containers (e.g., chlorine tanks) every 24 hours.	
	X	X		Establish unannounced security spot checks (e.g., verification of personnel identification and door security) at access control points for critical facilities	
	X	X		Conduct security audit of physical security assets, such as fencing and lights, and repair or replace missing/broken assets. Remove debris from along the fence lines that could be stacked to facilitate scaling.	
				Security Force	
	X	X		Patrol the inside fence line.	
	X	X		Institute random patrols	
	X	X		Assign security representatives to gate duty.	
	X	X		Deploy personnel at mission-critical sites	
				Cyber Security	
			X	Verify the security of critical information systems (e.g., supervisory control and the data acquisition, internet, e-mail, etc…) and review safe computer and internet access procedures with employees to prevent cyber intrusion.	

Exhibit 3 Protective Measures Implemented at HSAS Threat Level yellow Significant Risk of Terrorist Attack

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	Implement mailroom security procedures. Follow the guidance provided by the U.S. Postal Service.	
			X	Ensure that employees understand notification protocol in the event of a security breach.	
			X	Increase the frequency for posting employee reminders of the threat situation and about events that constitute security violations.	
				Incident Response	
			X	Review and update emergency response procedures and communication protocols.	
				Personnel Protection	
			X	Remind mailroom personnel of the need for heightened awareness and the use of personal protective gear when sorting and distributing all mail.	
			X	Periodically update personnel as the situation changes.	
				Infrastructure Interdependencies	
	X		X	Inspect all supporting infrastructure facilities (e.g., electric power, telecommunications) regularly.	

Exhibit 4 Protective Measures Implemented at HSAS Threat Level Orange High Risk of Terrorist Attack					
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		Employ stricter chemical delivery procedures.	
		X		Positively identify all employees entering the treatment facility.	
		X		Allow only essential personnel on-site.	
		X		Cancel facility tours.	
		X		Limit access points to utility facilities to the absolute minimum necessary for continued operations. Limit mission-critical facility access to essential employees and contractors.	
		X		Delay or stop construction at a mission-critical facility based on threat information and location of the work being preformed.	
		X		Keep front gate closed at all times and lock all other gates.	
		X		Restrict parking in the vicinity of the facility and critical assets.	
		X		Implement centralized parking and shuttle bus service as conditions warrant.	
		X		Close recreational areas and remove boats from reservoirs.	
		X		Tow unauthorized vehicles for the facility parking lots.	
				Barriers	
		X		Install anti-vehicle barriers (e.g., Jersey bounce, bollards).	
				Monitoring and Surveillance	
	X			Increase the use of CCTV video surveillance.	
	X	X		Install temporary lighting.	
	X			Increase water sampling	
	X			Increase the frequency and extent of monitoring activities and review the results against the baseline.	
				Communications	
		X	X	Confirm that counties and state health officials are on high alert and will inform water utilities of any potential water-borne illnesses.	
			X	Practice communications protocol with local authorities and others cited in the facility's emergency response plan.	
			X	Confirm that emergency response and laboratory analytical support networks are ready for deployment 24 hours a day, seven days a week.	
			X	Reaffirm liaison with local police, intelligence, and security agencies to determine the likelihood of an attack.	
				Inspection	
	X	X		Inventory Chemical containers (e.g., Chlorine tanks) regularly.	
	X	X		Inspect all dumpsters coming into the plant.	
	X	X		Perform regular perimeter checks.	
	X			Visually inspect all vehicles, including the undercarriage.	
				Security Force	
			X	Hire full time security personnel.	
		X	X	Install guard shack at the main entrance to the facility.	
	X	X		Implement roving security patrols in the buffer zone.	
				Cyber Security	
X			X	Ensure that mission-critical information is adequately protected and backed up.	
				Security Program	
	X	X	X	Ensure that water treatment/production facilities are staffed at all times.	
				Incident Response	
X				Limit the number of Chemical containers on site.	
				Personnel Protection	
			X	Update personnel on increased threat level.	
				Infrastructure Interdependencies	
	X		X	Inspect all supporting infrastructure facilities (e.g., electric power, telecommunications) daily	

Exhibit 5 Protective Measures Implemented at HSAS Threat Level Red Severe Risk of Terrorist Attack					
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		Discontinue tours and prohibit public access to all operational facilities.	
		X		Consider the need to prohibit all recreational use of surface water reservoirs.	
		X		Limit access to facilities and activities to essential personnel.	
		X		Inspect all employees and vehicles before they enter the facility.	
		X		Allow no commercial vehicles or deliveries inside the facility.	
		X		Use armed escort for essential shipments.	
		X		Relocate public meetings offsite.	
				Barriers	
		X		Employ jersey bounce, bollards, or pop-up barriers. Place in serpentine fashion at the front gate and other point of vehicular access.	
				Monitoring and Surveillance	
	X			Increase the frequency and extent of monitoring activities. Review results against the baseline.	
	X			Implement frequent and staggered inspections of the exterior of the building, to include roof and parking areas.	
	X		X	Consider requesting increased law enforcement surveillance, particularly of critical assets and otherwise unprotected areas.	
	X	X		Monitor all traffic in and around the facility and reroute street access.	
				Communications	
		X	X	Confirm that counties and health officials are on severe alert and will inform water utilities of any potential water-borne illnesses.	
			X	Practice communications protocol with local authorities and others cited in the facilities emergency response plan.	
			X	Reaffirm liaison with local police, intelligence and security agencies to determine the likelihood of an attack on the water system.	
			X	Ensure that employees are fully aware of emergency response communication protocols and have access to contact information for relevant law enforcement, public health, environment protection and emergency response organizations.	
			X	Ensure that list of sensitive populations (e.g., hospitals, schools, etc…) within the service area is accurate and shared with appropriate public health officials.	
			X	Where appropriate, provide public notification for citizens to store emergency water supply or to implement other preparatory measures.	
			X	Confirm that emergency response and laboratory analytical support networks are ready for deployment 24 hours a day, seven days a week.	
				Inspection	
	X			Recheck the security of all on-site chemical storage and utilization areas.	
	X	X		Conduct an inventory of containers every six hours.	
	X	X		Increase the use of helicopter fly-overs.	
	X	X		Inspect all carried baggage, such as suitcases, packages, and briefcases brought on to the facility for presence of explosives or incendiary devices or other dangerous items.	
				Security Force	
			X	Increase security patrol activity to the maximum level sustainable and ensure tight security in the vicinity of mission-critical facilities. Vary the timing of security patrols.	
			X	Place armed guards near chemical containers (e.g., Chlorine tanks) and elsewhere on the site.	
			X	Maintain a constant law enforcement presence.	
			X	Increase the number of roving security patrols in buffer zone.	
			X	Post armed guards with certified bomb-sniffing dogs at the site entrance or other checkpoints.	
			X	Activate or reassign available employees to ensure absolute control over access to critical facilities and other potential target areas.	
				Cyber Security	
			X	Request that employees change passwords on critical information management systems.	
			X	Recheck the security of the critical information systems (e.g., SCADA, internet, e-mail,etc…)	
				Security Program	
X			X	Consider whether mail and packages should go to a central, secure location and be inspected before distributing.	

Exhibit 5 Protective Measures Implemented at HSAS Threat Level Red Severe Risk of Terrorist Attack					
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**
				Incident Response	
			X	Ensure that the key utility personnel are on duty.	
			X	Consider placing staff at remote, typically unmanned, facilities.	
			X	Evaluate the need to open an emergency operations center.	
			X	Ensure that existing security policies and procedures are effectively implemented and that security equipment is properly utilized.	
			X	Request, as appropriate, increased law enforcement and/or security agency surveillance, particularly of critical assets and otherwise unprotected areas (e.g., consider if National Guard assistance is needed and make appropriate request).	
			X	Post city police at the facility, patrol high threat areas.	
			X	Divert interstate, rail and river traffic as appropriate.	
			X	Pre-position emergency response personnel to respond to HAZMAT incidents.	
			X	Limit hours of operation or close the facility.	
			X	Temporarily shut down chlorine operations.	
			X	Cancel or delay unnecessary employee travel and leave.	
				Personnel Protection	
			X	Provide security for personnel dispatched to repair or restore damaged facilities and systems.	
			X	Post daily notices to staff regarding the threat level and security practices.	
			X	Remind mailroom personnel of the need for heightened awareness when sorting and distributing all incoming mail.	
				Infrastructure Interdependencies	
X			X	Inspect and practice activation emergency interconnections with neighboring water agencies.	
X			X	Have an alternate water supply plan ready to implement (e.g., bottled water delivery).	
X			X	Where appropriate, place back-up operational capacity on line (filters, turbines, etc…)	

REFERENCES

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

1. U.S. Environmental Protection Agency, 2004, Guarding against Terrorist and Security Threats: Suggested Measures for Drinking Water and Wastewater Utilities (Water Utilities; available at: http://www.dhs.ca.gov/ps/ddwem/Homeland/Appendix/AppendixI_%20USEPAthreatlevelgucemarch_%2031.pdf
2. U.S. Environmental Protection Agency, 2004, Guarding against Terrorist and Security Threats: Suggested Measures (Wastewater Utilities); available at: http://krwa.org/docs/EPDGuarding WW.pdf
3. U.S. Environment Protection Agancy, 2003, Threat Advisory (Threat Level Orange); Available at: http://www.lgean.org/documents/threat_Advisory.pdf
4. Greenblat,M.J.Donohue, and K.Wagner, 2003, Homeland Security for drinking water supplies; available at: http://www.environmental-center.com/articles1264/article1264.htm

RESOURCES

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

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

Colorado Office of Preparedness and Security Homeland Security Section
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/