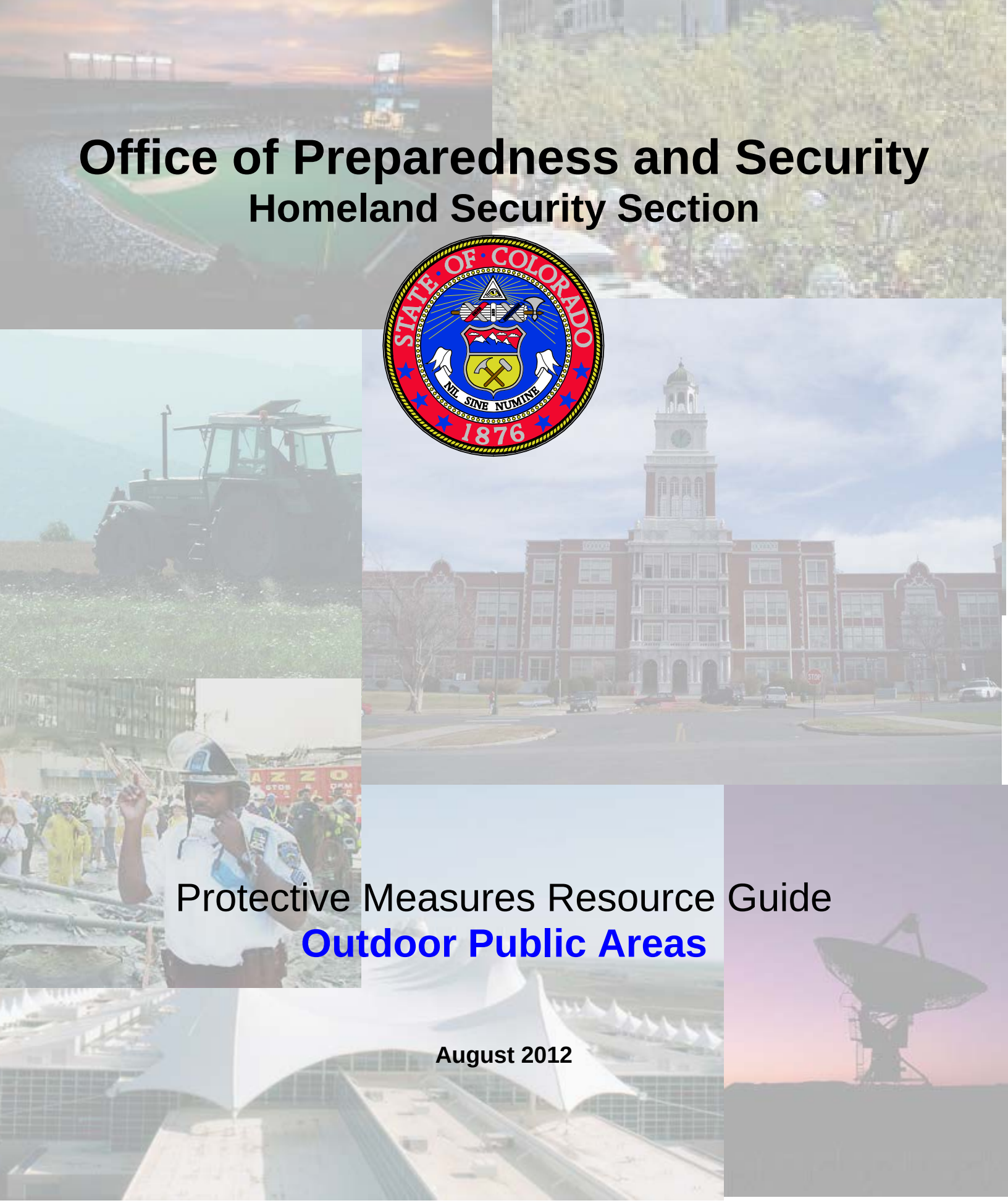
Office of Preparedness and Security
Homeland Security Section



Protective Measures Resource Guide
Outdoor Public Areas

August 2012

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

Protective measures are employed in order to:

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

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

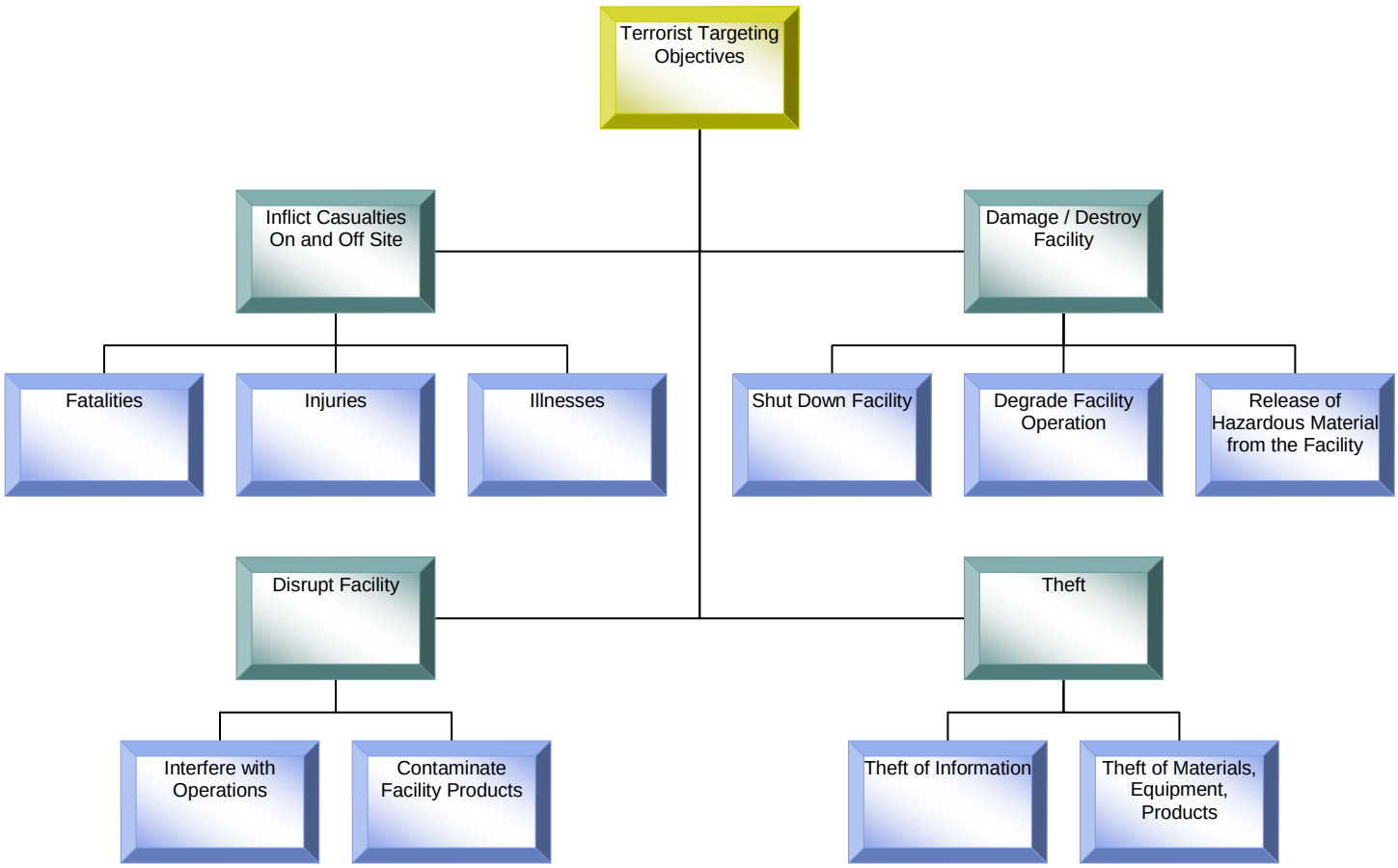
While a number of protective measures can be implemented for any of the critical infrastructure sectors, this guide is customized with protective measures for the following sector:

Infrastructure: Outdoor Public Gatherings

Criminal Objectives

In general terms, criminals 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 criminal attack on outdoor public areas.

Figure 1



Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many criminal 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

Criminals 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/criminals. 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/criminals 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/criminals 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

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

Sabotage

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

Assassination/Kidnapping

Assassinating key personnel or kidnapping individuals and taking hostages has been used in many criminalt 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 criminals; 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 Large Public Outdoor Gatherings are given on pages 10 and 11.

Available Protective Measures Matrix

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

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

Implementation of Protection Measures

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

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

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

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

When the available intelligence allows, the HSAS alerts are supplemented by information on a threat most likely to be used by criminals. 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 criminal 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 criminal event planning. While criminals are surveying 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 protective materials on pages 10 and11 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.

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

These suggestions should not be viewed as a complete source of information on protecting a particular function. Facility managers, function coordinators, 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.

Protective Measures for Outdoor Public Areas

Considerations:
Number of participants
Nature of event. (i.e., religious, political, transportation hubs)
Current HLS Threat Level

Access Control Measures

- Have participants pre-register to limit participation to pre-identified group members
- Issue identification credentials to participants to keep non-participants out (i.e., arm-bands, bracelet, electronic ID tags, number placard on shirt etc...)

Barriers

- Set up barricades and/or fencing to control entry and exit to event to establish choke points for security screening
- Set up concrete barriers to protect venue from car bombing

Communications

- Equip event staff with communications equipment (cellular phones, handheld radio) considering that cell phones towers may be overloaded in a disaster
- Develop public address system to address crowd
- Equip event staff supervisors with hand held megaphones for emergency communications

Inspection

- Prior to choosing event location, request assistance from the Homeland Security Officer from local law enforcement
- Identify vulnerabilities
- Choose a site that best protects participants from criminal attacks

Security Forces

- Hire uniformed police officers to patrol venue and surrounding areas
- Have uniformed police or private security staff guard vulnerable infrastructure (refreshments, HVAC, gathering areas, vehicle drop off areas)
- Lockdown or paint manhole or utility covers in the area to identify those areas that are vulnerable and need to be monitored

Cyber Security

- If using online registration, work with computer system administrator to protect personal information from hackers
- Set up computer logs to monitor attempts to hack site
- Do not store critical security information such as site diagrams, maps, staffing schedules on computers with open access to the internet

Incident Emergency Response Measures

- Hire ambulances to be on standby in the venue area
- Prepare credentials for event staff and vendors
- Purchase required permits from municipal authority
- Ensure venue meets fire protection and access requirements
- Request patrol by Bomb Detection K9
- Request notification by Municipal authority if the following occur prior to event:
    - A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
    - Increase in power outages
    - Displaced manhole covers
    - Unusual maintenance activities (road repairs etc.) in the area

- Prepare Emergency Plan for event: cover;
  - How to cancel the event if HLS color threat level increases or suspicious activity is observed
  - Triage of mass casualty victims if criminal attack occurs
  - Plan to communicate emergency information to a panicked crowd
  - Identification of a public information officer
  - Identification of event emergency manager
  - Method of event staff communicating in case of emergency and cell phone failure

Personal Protection

- Develop Written Emergency Procedures for common threats (i.e., bomb Threat, Fire, Severe Weather, Assault, Counter Demonstrators, etc…)

Infrastructure Interdependencies

- Avoid locating critical infrastructure in same locations (electric, phone communications, parking area)
- Put up fencing around temporary hookups, generators, radio equipment etc…

Event Staff Training

- Educate staff on nature of threats the event may face.
- Identify Current Homeland Security Threat Level and determine if it still safe to hold the event.
- Consider rules regarding prohibiting or inspecting packages or backpacks into the venue area.
- During event planning and setup stages be observant for the following:
  - Persons in the area wearing military style clothing or carrying military style weapons or equipment
  - Persons videotaping or photographing the venue, event equipment or event personnel
  - Persons parking, standing or loitering in the same area over a multiple day period
  - Event staff being questioned off site, or phone calls and inquiries about practices or procedures pertaining to the event
  - People wearing clothing that is not consistent with local weather
  - Attempts to hack into the event website
  - Use computer logs to monitor access to personal information, maps or other targeting information
    - If any of these events are observed notify the Homeland Security Officer for the local jurisdiction (Provide; description, name if known, vehicle license plate etc...)

The day of the event

- Have abandoned vehicles or trucks towed from the area
- Notify all participants to watch for abandoned backpacks or packages
- Be observant to lack of insects, dead birds or dead small animals
- Watch for people wearing clothing that is not consistent with local weather
- Station security personnel to protect refreshments from tampering
- Station security personnel to protect HVAC systems, trash cans (located near places where people congregate, etc…)
- Watch for maintenance events (road repair, telephone service etc…) which were not scheduled
- Have security personnel search and inspect vendor vehicles and trailers before they are brought into venue

REFERENCES

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

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

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

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

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

RESOURCES

SPECIAL EVENT REFERENCES

http://www.publicvenuesecurity.com
http://www.iccsafe.org
http://www.kdl.to/guides/event-safety-planning-guide.htm
http://www.iaam.org/Facility_manager/Pages/2002_Jan_Feb/Feature_7.htm
http://www.iaam.org/Facility_manager/Pages/Facility_Issues.htm
http://www.ci.milpitas.ca.gov/citydept/fire/fireprev/nightclub_fire.pdf
http://training.fema.gov/EMIWeb/IS/is15.asp

REFERENCE

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

TRADE PUBLICATIONS

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

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

http://www.contingencyplanning.com/ industry magazine

http://www.contingencyplanning.com/e-newsletters/index.aspxsubscribe to e newsletter
http://www.contingencyplanning.com/archives/index.aspx reference to past articles
http://www.infosyssec.net/index.html information security
http://infosyssec.tradepub.com/_brands/infosyssec/cat/Info.cat.html free publications for industry

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

TRAINING/CERTIFICATION

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

http://www.thebci.org/mainindex.htm offers training and professional certification for industry (non profit)

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

GOVERNMENT AGENCIES

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

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

http://www.redcross.org/

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

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

http://www.dhs.gov/dhspublic/ Department of Homeland Security
https://www.llis.dhs.gov/ Lessons learned

CONTACT INFORMATION

Colorado Office of Prevention and Security
Homeland Security Section
690 Kipling Street, #2100
Lakewood, Co., 80215
720-852-6705
CIAC@CIAC.CO.GOV