

2009 HOSPITALITY LAW CONFERENCE

Hotels: Common Vulnerabilities, Potential Indicators of Terrorist Activity, & Protective Measures





Presenter



- **Bill Schweigart, Department of Homeland Security**
- Program Analyst for the Office of Infrastructure Protection, Commercial Facilities Sector
- Focus is on the Lodging, Entertainment & Media, Real Estate, and Cultural Properties
- Former U.S. Coast Guard officer with a background in Continuity of Operations (COOP) planning, critical infrastructure protection, and pandemic planning



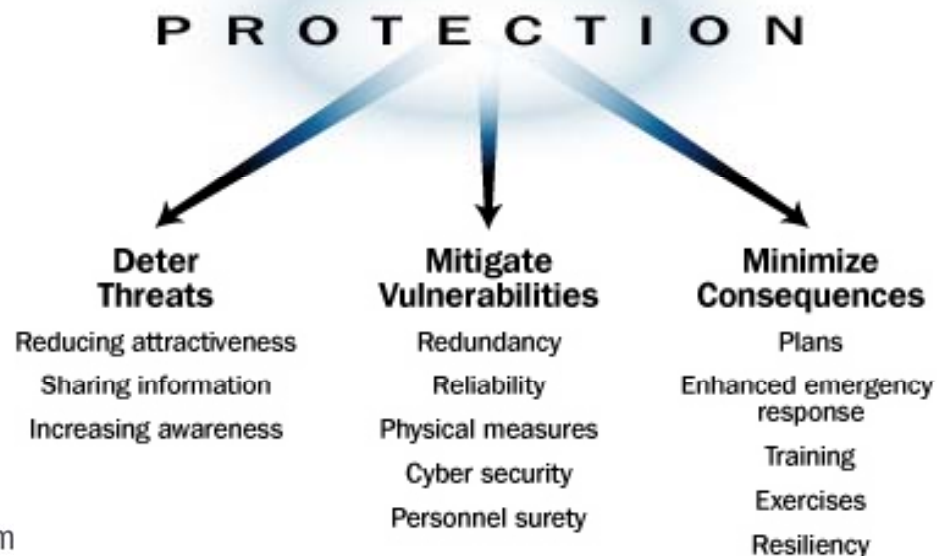
Agenda

- The Commercial Facilities Sector
- Hotels: Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures
- DHS Protective Programs



National Infrastructure Protection Plan

- *Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and strengthening national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.*





Commercial Facilities Sector

The Commercial Facilities Sector comprises a number of segments. The diversity of assets within the sector leads to a myriad of activities being performed within. Facilities within this sector are generally designed for one of the following purposes:

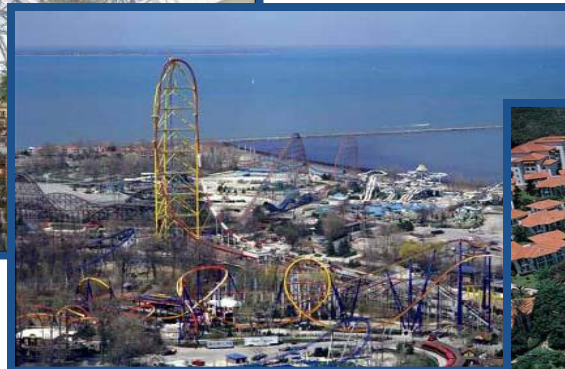
Business Activities



Personal Commercial Transactions



Recreational Pastimes



Accommodations



**Homeland
Security**



Commercial Facilities Sector Functional View

Public Assembly	Sports Leagues	Resorts	Lodging	Outdoor Events	Entertainment and Media	Real Estate	Retail
<ul style="list-style-type: none"> •Movie Theatres •Convention Centers •Performing Arts Centers •Zoos •Aquariums •Museums •Stadiums •Arenas 	<ul style="list-style-type: none"> •Arenas •Stadiums •Horse Racing Tracks •Auto Racing Tracks •Professional and Amateur Sports Leagues 	<ul style="list-style-type: none"> •Casinos •Hotels •Conference Centers •Arenas •Shopping Malls 	<ul style="list-style-type: none"> •Hotels •Conference Centers 	<ul style="list-style-type: none"> •Amusement Parks •Fairs •Exhibitions •Outdoor Events •Hotels 	<ul style="list-style-type: none"> •Production Studios (TV & Movie) •Broadcast Studios (TV & Radio) •Print Media •Transmission •Hotels 	<ul style="list-style-type: none"> •Office Buildings •Industrial Buildings •Multi-Family Towers & Condos •Self Storage Facilities 	<ul style="list-style-type: none"> •Retail Centers •Shopping Malls •Movie Theatres •Stand-Alone Retail Stores



Agenda

- The Commercial Facilities Sector
- Hotels: Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures
- DHS Protective Programs



Terrorist Targeting Objectives

- **Inflict Casualties**
 - Fatalities
 - Injuries
 - Illnesses
- **Damage/Destroy Facility**
 - Shut down facility
 - Degrade Facility Operation
 - Release hazardous material from facility
- **Disrupt Facility**
 - Interfere with operations
 - Contaminate facility products
- **Theft**
 - Theft of materials, equipment, products
 - Theft of information



Specific Terrorist Threats

- **Explosives** (e.g., car bomb, suicide bomber)
- **Arson** (e.g., firebombing, use of accelerants)
- **Biological agents** introduced into the facility (e.g., anthrax, botulism)
- **Chemical agents** introduced into the facility (e.g., chemical warfare agents, toxic industrial chemicals)
- **Radiological material** introduced into the facility
- **Hostage taking**
- **Automatic weapons or grenade attack** (e.g., indiscriminate shooting of patrons)
- **Theft** of proprietary or sensitive information



Impacts and Effects of an Attack

- Potential for many casualties – bombing, release of CBR agent, structural collapse, smoke/dust inhalation, stampeding crowds
- Economic losses of hotels owners, insurance companies, lost jobs, etc.
- Psychological impact across America; decreased travel and tourism nationwide



Definition of Common Vulnerabilities

- Common vulnerabilities to terrorist activity have generally been observed or are known to generally exist within an infrastructure category.
- Critical infrastructures and key assets vary in many characteristics and practices relevant to specifying vulnerabilities.
- There is no universal list of vulnerabilities that applies to all assets of a particular type within an infrastructure category.
- “Common” vulnerabilities should be interpreted as having a high likelihood of occurrence, but not as applying to each and every individual facility or asset.



Common Vulnerabilities: Hotels



- Guest drop-off and pick-up points that may not be distant enough to mitigate blasts from explosives in vehicles
- Parking garages may have open access to the public with little to no screening
- Many hotels have a limited security force

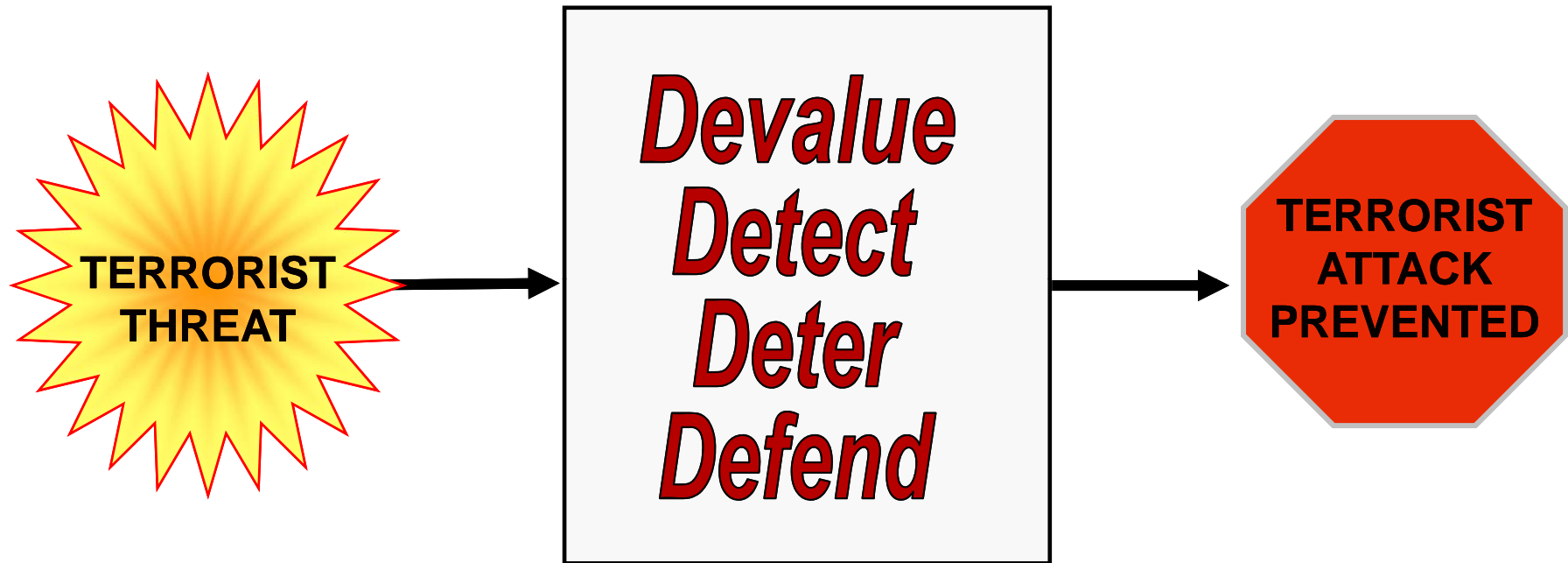


Potential Indicators of Terrorist Activity

- Potential Indicators of surveillance may include:
 - Persons discovered with a suspicious collection of casino/hotel maps, photos, or notes or diagrams with infrastructure highlighted
 - Personnel being questioned off-site about practices pertaining to the facility or the facility's supporting infrastructure (e.g., electricity and natural gas lines)
 - Theft of employee or contractor ID cards or uniforms
 - A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Observable anomalies or incidents that may be indicators of an imminent attack:
 - Persons in crowded areas wearing unusually bulky clothing
 - Unattended vehicles illegally parked near entrance, exit areas, or places where large numbers of patrons gather
 - Unattended packages (e.g., backpacks, briefcases, boxes or luggage)
 - Indications of unusual substances near air intakes



Protective Measures



**A coordinated effort by the Private Sector and
Federal, State, and Local Governments**



Protective Measures Include:

- Planning and Preparedness
 - Designate a security director
 - Conduct threat analyses, vulnerability assessments, consequence analysis, risk assessments and security audits on a regular basis
- Cyber Security
 - Develop and implement a security plan for computer hardware and software
- Personnel
 - Conduct background checks on employees
 - Incorporate security awareness into employee training programs



Protective Measures Include:

- Access Control
 - Photo identification badges for employees
- Barriers
 - Install building perimeter barriers (sculptures, flower pots, fences, bollards, shallow ditches, high curbs)
- Monitoring & Surveillance
 - Install and monitor CCTV systems
- Communications
 - Install systems that provide communication with all people at the facility, and can work in concert with law enforcement and emergency responders
- Incident Response
 - Identify alternate rallying points for coordinated evacuations



Agenda

- The Commercial Facilities Sector
- Hotels: Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures
- DHS Protective Programs



DHS Protective Programs

- Homeland Security Information Network
- Protective Security Advisors (PSAs)
- Site Assistance Visits (SAVs)
- Common Vulnerabilities (CV), Potential Indicators of Terrorist Activities (PI), and Protective Measures (PM) Reports
- FEMA 452
- Protect Your Workplace Campaign
- BMAP Suspicious Behavior Awareness
- Active Shooter Materials
- Awareness Training
- Protected Critical Infrastructure Information (PCII) Program
- *Protective Measures Guide for the U.S. Lodging Industry*



HSIN

- The Homeland Security Information Network (HSIN) is a secure portal that provides a “peer to peer” collaboration space for members to engage in real-time.
- The each Subsector has its own sub-portal within the CF portal.
- Resources available on HSIN include Joint Information Bulletins issued by DHS and the FBI.

HSIN-CFS COMMERCIAL FACILITIES SECTOR

My Site Help

Home Sectors Daily OSIR US-CERT User Information

Current Location [Home](#) > Sectors > Commercial Facilities

Current Location

- Home
- Sectors
 - Commercial Facilities
 - Documents
 - Discussions
 - Sites
 - Administration

Actions

- Add Listing
- Add Person
- Upload Document
- Change Settings
- Manage Content
- Manage Portal Site
- Add to My Links
- Alert Me
- Edit Page

Commercial Facilities Announcements

Severity Title Created By Modified Body

There are no items to show in this view of the "Commercial Facilities Announcements" list. To create a new item, click "New item" above.

Events

There are currently no upcoming events. To add a new event, click "Add new event" below.

[Add new event](#)

Recently Updated Documents

More than 10 results, showing items 1 - 10

Sort by [Date \(newest first\)](#) then group by [Date](#) | [Add to My Links](#) | [Alert Me](#)

Type	Name	Modified	Modified by	Size
Document	Region 6 Critical Infrastructure Protection Plan- ...	Today	christa.cole@metrokc.gov	17 KB
Document	DHS Open Source Infrastructure Report 2007-05-02	Today	Alfred Brownley1	97 KB

Commercial Facilities Hot Site Links

- Sector Coordinating Council Working Group
- Demonstration Site for CF Sector

Jabber

HSIN Jabber
CHAT COMMUNICATION

Click the above logo to access the real-time HSIN Jabber chat communication tool. Full Jabber Thick client may be downloaded [here](#).

Contacts (click for more information)



Protective Security Advisors

- PSAs are assigned to local communities throughout the U.S. They serve as DHS liaisons between the private sector and Federal, State, Territorial, local, and tribal governments.
- PSAs assist in identifying critical infrastructure and key resource assets.
- PSAs coordinate requests by the private sector for DHS services and resources, including training requests and scheduling of SAVs.
- PSA Duty Desk: **703-235-5724**



Site Assistance Visits

- SAVs are visits to critical infrastructure facilities led by DHS protective security professionals, in conjunction with subject-matter experts and local law enforcement.
- SAVs are designed to facilitate vulnerability identification and mitigation discussions between DHS and the facility in the field.
- The focus of the SAV is evolving from vulnerability to a broader risk-based assessment by analyzing consequences and incorporating threat scenarios.
- SAVs have been performed at 5 different amusement, theme and water park venues across the United States.



Three Types of Reports Have Been Developed For Each Infrastructure and Facility Category

Increase Awareness & Improve Understanding

Characteristics and Common Vulnerabilities



- Common characteristics, components, and applicable standards
- Consequences of events
- Common vulnerabilities

Potential Indicators of Terrorist Activity



- Terrorist targeting objectives
- Activity indicators

Protective Measures



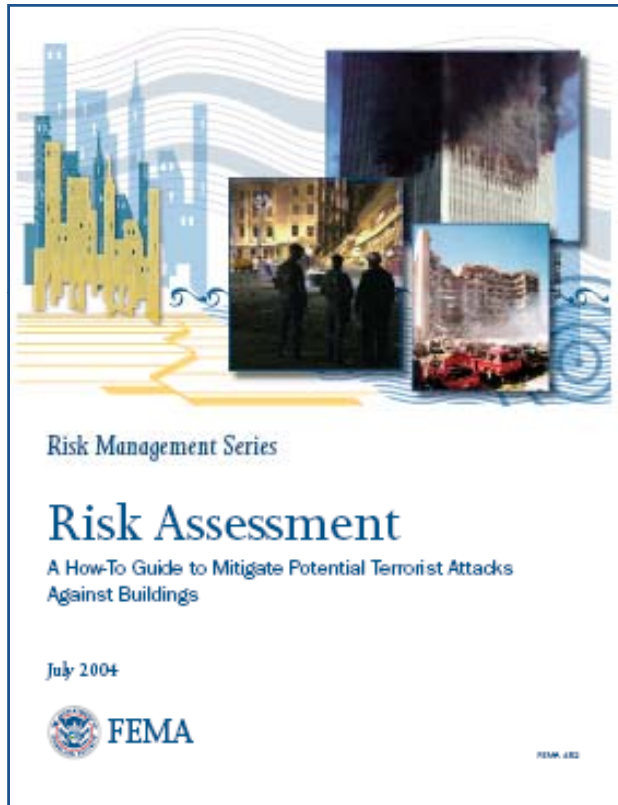
- Methods for:**
- Increasing awareness
 - Reducing vulnerabilities
 - Enhancing defense

Condensed, comprehensive reports are available for performance venues and shopping malls at

<https://cvpipm.iac.anl.gov>



FEMA 452



- The FEMA 452 risk assessment methodology is founded on
 - conducting an asset value assessment
 - threat identification and rating
 - vulnerability assessment
 - coming up with mitigation options to reduce the highest risk
 - then making risk management decisions.
- Currently the threats addressed in FEMA 452 are include explosive blast and CBR
 - Currently being updated to include:
 - Floods
 - High Winds
 - Earthquakes



“Protect Your Workplace” Campaign

- “Protect Your Workplace” is a poster campaign designed to build security awareness among the American workforce.
- The 4 posters offer various physical and cyber security guidelines.
- Since 2006, more than 105,000 posters and brochures have been downloaded from the US-CERT Web site (www.us-cert.gov/reading_room/distributable.html), reaching more than 20,000 workplaces.



“Protect Your Workplace” Posters

www.us-cert.gov/reading_room/distributable.html

Protect Your Workplace

Cyber Security Guidance

Employees

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your user names, passwords, or other computer/website access codes to anyone.
- Do NOT open e-mails or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
- Make electronic and physical back-ups or copies of all your most important work.
- Report all suspicious or unusual problems with your computer to your IT department.

Management & IT Department

- Implement Defense-in-Depth: a layered defense strategy that includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.

Report a computer or network vulnerability to the U.S. Computer Emergency Response Team Incident Hotline: 1-888-282-0870

www.US-CERT.gov

For more cyber tips, best practices, "how-to" guidance, or sign up for our bi-weekly and semi-technical cyber alerts, visit our download site page: www.US-CERT.gov

Report Suspicious Cyber Incidents

SYSTEM FAILURE OR DISRUPTION
Has your system or website's availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

UNAUTHORIZED CHANGES OR ADDITIONS
Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent?

SUSPICIOUS QUESTIONING
Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware?

SUSPICIOUS E-MAILS
Are you aware of anyone in your organization receiving suspicious e-mails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

UNAUTHORIZED ACCESS
Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or its data?

UNAUTHORIZED USE
Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

We encourage you to report any activities that you feel meet these criteria for an incident. Note that our policy is to keep any information specific to your site and names confidential unless we receive your permission to release that information. US-CERT has partnered with law enforcement agencies such as the U.S. Secret Service and the Federal Bureau of Investigation to investigate cyber incidents and prosecute cyber criminals.

Report an incident to the U.S. Computer Emergency Response Team Incident Hotline: 1-888-282-0870

www.US-CERT.gov

For more cyber tips, best practices, "how-to" guidance, or sign up for our bi-weekly and semi-technical cyber alerts, visit our download site page: www.US-CERT.gov

Protect Your Workplace

Physical Security Guidance

- Monitor and control who is entering your workplace: current employees, former employees, and commercial delivery and service personnel.
- Check identification and ask individuals to identify the purpose of their visit to your workplace.
- Report broken doors, windows, and locks to your organization's or building's security personnel as soon as possible.
- Make back-ups or copies of sensitive and critical information and databases.
- Store, lock, and inventory your organization's keys, access cards, uniforms, badges, and vehicles.
- Monitor and report suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, garages, and immediate vicinity.
- Report suspicious-looking packages to your local police. DO NOT OPEN or TOUCH.
- Shred or destroy all documents that contain sensitive personal or organizational information that is no longer needed.
- Keep an inventory of your most critical equipment, hardware, and software.
- Store and lock your personal items such as wallets, purses, and identification when not in use.

Call your local police department to report a suspicious person, vehicle, or activity in or near your workplace.

Call 911 if it is an emergency.

To download this poster, visit www.US-CERT.gov

Report Suspicious Behavior and Activity

SURVEILLANCE
Are you aware of anyone recording or monitoring activities, taking notes, using cameras, maps, binoculars, etc., near a key facility?

TESTS OF SECURITY
Are you aware of anyone attempting to penetrate or test physical security or procedures at a key facility?

ACQUIRING SUPPLIES
Are you aware of anyone attempting to improperly acquire explosives, weapons, ammunition, dangerous chemicals, uniforms, badges, flight manuals, access cards, or identification for a key facility or to legally obtain items under suspicious circumstances that could be used in a terrorist act?

DRY RUNS
Have you observed any behavior that appears to be preparation for terrorist activity, such as mapping out routes, playing out scenarios with other people, monitoring key facilities, timing traffic lights or traffic flow, or other suspicious activities?

DEPLOYING ASSETS
Have you observed abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility?

SUSPICIOUS PERSONS
Are you aware of anyone who does not appear to belong in the workplace, neighborhood, business establishment, or near a key facility?

SUSPICIOUS QUESTIONING
Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding a key facility or its personnel?

Call 911 if there is an emergency or immediate threat. Call the nearest Joint Terrorism Task Force (JTTF) to report suspicious activity or behavior (see below). Submit information electronically at info.jtffs.fbi.gov

Alaska (907) 487-1311	Colorado (303) 455-2000	Florida (888) 357-3772	Illinois (815) 462-5000	Missouri (816) 425-2000
Arizona (602) 354-1300	Connecticut (860) 424-3000	Georgia (404) 521-5000	Indiana (317) 232-2000	Montana (406) 442-2000
Arkansas (501) 475-0800	Delaware (302) 424-3000	Hawaii (808) 521-5000	Iowa (515) 281-2000	Nebraska (402) 475-2000
California (916) 434-0800	District of Columbia (202) 452-5000	Idaho (208) 333-2000	Kansas (785) 843-2000	Nevada (702) 438-2000
Colorado (303) 455-2000	Florida (888) 357-3772	Kentucky (502) 221-2000	Michigan (517) 487-2000	New Hampshire (603) 271-2000
Connecticut (860) 424-3000	Georgia (404) 521-5000	Louisiana (504) 383-2000	Minnesota (612) 676-2000	New Jersey (908) 291-2000
Delaware (302) 424-3000	Hawaii (808) 521-5000	Maine (207) 624-2000	Mississippi (601) 359-2000	New Mexico (505) 325-2000
District of Columbia (202) 452-5000	Idaho (208) 333-2000	Maryland (410) 326-2000	Montana (406) 442-2000	New York (914) 337-2000
Florida (888) 357-3772	Illinois (815) 462-5000	Massachusetts (617) 552-2000	Nebraska (402) 475-2000	North Carolina (919) 435-2000
Georgia (404) 521-5000	Indiana (317) 232-2000	Michigan (517) 487-2000	Nevada (702) 438-2000	North Dakota (701) 785-2000
Hawaii (808) 521-5000	Iowa (515) 281-2000	Minnesota (612) 676-2000	New Hampshire (603) 271-2000	Ohio (614) 439-2000
Idaho (208) 333-2000	Kansas (785) 843-2000	Mississippi (601) 359-2000	New Jersey (908) 291-2000	Oklahoma (405) 521-2000
Illinois (815) 462-5000	Kentucky (502) 221-2000	Montana (406) 442-2000	New Mexico (505) 325-2000	Oregon (503) 463-2000
Indiana (317) 232-2000	Louisiana (504) 383-2000	Nebraska (402) 475-2000	New York (914) 337-2000	South Carolina (803) 799-2000
Iowa (515) 281-2000	Maine (207) 624-2000	Nevada (702) 438-2000	North Carolina (919) 435-2000	South Dakota (605) 781-2000
Kansas (785) 843-2000	Maryland (410) 326-2000	New Hampshire (603) 271-2000	North Dakota (701) 785-2000	Tennessee (615) 251-2000
Kentucky (502) 221-2000	Massachusetts (617) 552-2000	New Jersey (908) 291-2000	Ohio (614) 439-2000	Texas (817) 798-2000
Louisiana (504) 383-2000	Michigan (517) 487-2000	New Mexico (505) 325-2000	Oklahoma (405) 521-2000	Utah (801) 468-2000
Maine (207) 624-2000	Minnesota (612) 676-2000	Oregon (503) 463-2000	Oklahoma (405) 521-2000	Virginia (800) 368-5898
Maryland (410) 326-2000	Mississippi (601) 359-2000	South Carolina (803) 799-2000	Oregon (503) 463-2000	Washington (206) 462-2000
Massachusetts (617) 552-2000	Montana (406) 442-2000	South Dakota (605) 781-2000	South Carolina (803) 799-2000	Washington (206) 462-2000
Michigan (517) 487-2000	Nebraska (402) 475-2000	Tennessee (615) 251-2000	Tennessee (615) 251-2000	Washington (206) 462-2000
Minnesota (612) 676-2000	Nevada (702) 438-2000	Texas (817) 798-2000	Texas (817) 798-2000	Washington (206) 462-2000
Mississippi (601) 359-2000	New Hampshire (603) 271-2000	Utah (801) 468-2000	Utah (801) 468-2000	Washington (206) 462-2000
Montana (406) 442-2000	New Jersey (908) 291-2000	Virginia (800) 368-5898	Virginia (800) 368-5898	Washington (206) 462-2000
Nebraska (402) 475-2000	New Mexico (505) 325-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Nevada (702) 438-2000	New York (914) 337-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
New Hampshire (603) 271-2000	North Carolina (919) 435-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
New Jersey (908) 291-2000	North Dakota (701) 785-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
New Mexico (505) 325-2000	Ohio (614) 439-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
New York (914) 337-2000	Oklahoma (405) 521-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
North Carolina (919) 435-2000	Oregon (503) 463-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
North Dakota (701) 785-2000	South Carolina (803) 799-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Ohio (614) 439-2000	South Dakota (605) 781-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Oklahoma (405) 521-2000	Tennessee (615) 251-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Oregon (503) 463-2000	Texas (817) 798-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
South Carolina (803) 799-2000	Utah (801) 468-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
South Dakota (605) 781-2000	Virginia (800) 368-5898	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Tennessee (615) 251-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Texas (817) 798-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Utah (801) 468-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Virginia (800) 368-5898	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000
Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000	Washington (206) 462-2000



BMAP Suspicious Behavior Awareness Cards

- BMAP outreach materials will be comprised of memorable, concise tips and images related to identifying and reporting HME and IED precursor materials and suspicious behavior.



FBI-DHS

Private Sector Advisory



Businesses can become unwitting participants in illicit or terrorist activities. Be aware of unusual or suspicious purchases or usage of your products and services. See reverse for details.

What can you do? Follow these simple steps:

- Understand how your products and services may be used illicitly
- Discuss product or service usage with customers and suggest alternatives
- Ask for customer ID and maintain a log of suspicious purchases
- Know your customers and report suspicious activity to authorities

Concerned? Contact local authorities for more information:


Local Police: _____

Local FBI Office: _____




Know your customers. Be aware. Your effort makes a difference.

Suspicious behavior card- front









FBI-DHS

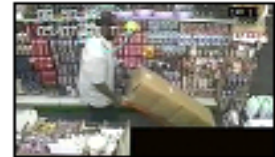
Private Sector Advisory




What are common examples?

-  Nervous or evasive customer attitude
-  Vague knowledge of a product's proper use
-  Requests for unusual product quantities
-  Refusal to purchase or utilize recommended substitutes
-  Insistence on in-store pick-up for bulk purchases
-  Large cash purchases

Know your customers. Be aware. Your effort makes a difference.



CC TV captures show foreign terrorist purchasing over quantity of hydrogen peroxide that was used in London attacks

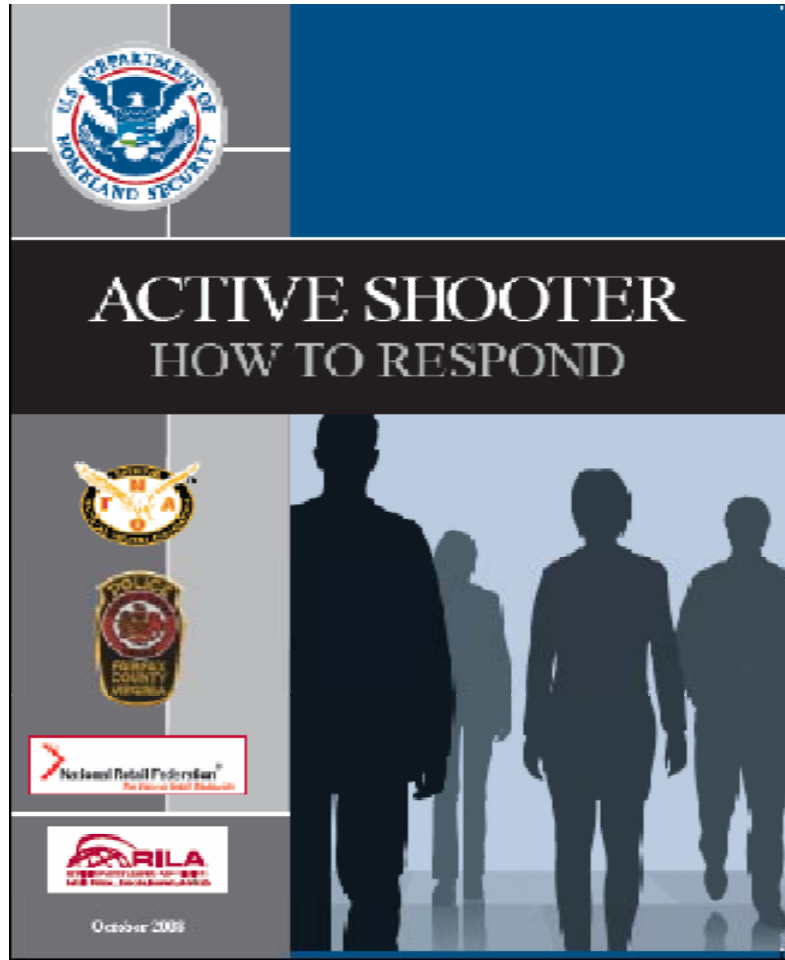


Surveillance footage shows terrorist moving bulk quantities of acetone into commercial storage facilities for use in attacks

Suspicious behavior card- reverse



Active Shooter Training & Outreach Materials



- Provide private sector partners with the tools needed to aid in preparing for and training for an Active Shooter Incident
- Materials consist of 3 products
 - Basic Guide Book
 - Break Room Poster
 - Pocket Emergency Measures Guide



DHS Awareness Training

Soft Target Awareness Course

- This 4-hour course offers individual training modules on terrorism awareness that are geared toward stadiums/arenas, places of worship, malls and shopping centers, theme parks, and large buildings

Surveillance Detection Training

- This 3-day course the process on developing Surveillance Detection plans and employing this protective measure to detect and deter potential threats to CI/KR

Private Sector Counterterrorism Awareness Workshop

- This 1-day course is designed to improve the knowledge of Private Sector security professionals by providing exposure to key elements of soft target awareness, surveillance detection, and improvised explosive device (IED) recognition

Protective Measures Course

- This 2-day course, offered to Executive Level and Employee Level Personnel in the private sector, is designed to provide students with the knowledge to identify vulnerabilities and select appropriate Protective Measures for their unique facility



The SAFETY Act

- The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) was enacted as part of the Homeland Security Act of 2002
- Intended to facilitate the development and deployment of anti-terrorism technologies by creating systems of “risk management” and “litigation management”
- Protections apply only to claims arising out of, relating to, or resulting from an act of terrorism.



Benefits of SAFETY Act Designation

- Exclusive action in Federal court
- No joint and several liability for non-economic damages
- No punitive damages or prejudgment interest
- Plaintiff's recovery reduced by amounts from collateral sources



Who Is Eligible?

- The SAFETY Act liability protections apply to a vast range of technologies, including:
 - Products
 - Services
 - Software and other forms of intellectual property



Who are the SAFETY Act Reviewers?

- Approximately 420 experts available to review applications.
- Conflict of Interest & Non-Disclosure Agreement signed by each reviewer per application.
- Three Technical Reviewers and two Economic Reviewers per application.
- Reviewers from the FFRDCs, Federal Government, Federal & National Labs, and Academia.
- 100+ trained reviewers (SMEs) in:

Cyber Chemical Radiological/Nuclear
Economic Biological Explosives Human Services



How to Apply for SAFETY Act Designation

- The SAFETY Act application kit with instructions and forms may be found and completed at **www.safetyact.gov**
- This site also contains information on the SAFETY Act statute and other reference materials.
- Cost = \$0.00



The PCII Program

- The Critical Infrastructure Information Act of 2002 protects voluntarily submitted critical infrastructure information from public disclosure under:
 - Freedom of Information Act (FOIA)
 - State and local sunshine laws
 - Civil litigation proceedings
- The Protected Critical Infrastructure Information (PCII) Program is an information-protection program designed by DHS to enhance information sharing between private sector and government. Information protected under PCII cannot be used for regulatory purposes.



PCII Protection

- Info designated as PCII is protected throughout its lifecycle.
- Protection extends to drafts and copies of the PCII retained by the submitter(s) or person working with the submitter(s), as well as any discussions with DHS regarding the PCII.
- The PCII Program safeguards ensure that PCII is:
 - Accepted only by authorized and properly trained individuals;
 - Used appropriately for analysis of threats, vulnerabilities, and other homeland security purposes;
 - Protected from disclosure under FOIA and other similar State and local disclosure laws; and
 - Not used directly in civil litigation nor as the basis for regulatory action.



How is PCII Shared?

- Directly through the PCII Program Office
- Through DHS field representatives and other Federal agencies designated to receive PCII by the PCII Program Manager



How To Participate in PCII

- Consider your existing information sharing relationships and how protection offered by the PCII Program could benefit your organization
- Identify CII held by your organization that could be of use for homeland security purposes
- Contact PCII Program Office staff with questions or for guidance on submitting information for protection:

PCII Program Office
Department of Homeland Security
245 Murray Lane, SW, Building 410
Washington, DC 20528-0001
202-360-3023
www.dhs.gov/pcii
pcii-info@dhs.gov



Protective Measures Guide for the U.S. Lodging Industry

- Commercial Facilities would like to initiate a collaborative effort to develop a *PMG for the U.S. Lodging Industry*
 - Overview of protective measures to assist Lodging owners/operators in planning and managing security at their facilities
 - A compilation of the materials shared with the CF Sector and intended for reference and guidance purposes only
 - Ideal for facilities without robust protective measures and/or emergency action plans in place who benefit from the expertise of their industry partners
- Similar to *Protective Measures Guide for U.S. Sports Leagues*
- Next steps: 1-on-1 engagement, security guides, and protective measures recommendations



Commercial Facilities Sector Vision Statement

The Commercial Facilities Sector envisions a secure, resilient, and profitable sector in which **effective and non-obstructive** risk management programs instill a positive sense of safety and security in the public and **sustain favorable business environments** conducive to attracting and retaining employees, tenants, and customers.





Office of Infrastructure Protection Contact Information:

Dave Crafton
Branch Chief, Commercial Facilities Sector
(202) 282-8249
Wilson.Crafton@dhs.gov

Andrea T. Schultz
Deputy Branch Chief, Commercial Facilities Sector
(703) 235-5768
Andrea.Schultz@dhs.gov

Bill Schweigart
Program Analyst, Commercial Facilities Sector
(703) 605-0648
Bill.Schweigart@dhs.gov



Questions?



Homeland Security