Session Handouts

Safe and Secure
Keeping our Spaces

Open Source Play, Sharing the Creative Code

Interactivity 2018
SUMMARY OF TERRORISM THREAT TO THE U.S. HOMELAND
Since 2015, the Department of Homeland Security (DHS) has used this Bulletin to highlight the continuing terror threat to the U.S. Homeland. The United States is engaged in a generational fight against terrorists who seek to attack the American people, our country, and our way of life. An informed, vigilant and engaged public remains one of our greatest assets to identify potential terrorists and prevent attacks.

ADDITIONAL DETAILS
- We continue to face one of the most challenging threat environments since 9/11, as foreign terrorist organizations exploit the Internet to enable, or direct individuals already here in the homeland to commit terrorist acts. Homegrown terror suspects increasingly rely on technology, such as end-to-end encrypted social media applications, to avoid detection.
- Terrorist groups are urging recruits to adopt easy-to-use tools to target public places and events. Specific attack tactics have included the use of vehicle ramming, small arms, straight-edged blades or knives, homemade explosives, and poisons or toxins.
- Some terrorist groups overseas are using battlefield experiences to pursue new technologies and tactics, such as unmanned aerial systems and chemical agents that could be used outside the conflict zones. Additionally, terrorists continue to target commercial aviation and air cargo, including with concealed explosives.
- Violent extremist media encourages individuals worldwide to launch attacks using all means possible. Continued U.S. and partner successes in disrupting and defeating terrorists on the battlefield may encourage homegrown terrorists to carry out acts of violence in the homeland instead of attempting to travel overseas to fight or in retaliation for apparent losses.
- Additionally, foreign terrorist fighters who have acquired training and battle-tested terrorism experience may flee from terrorist-controlled territories with a desire to conduct attacks elsewhere, including the United States.

U.S. GOVERNMENT COUNTERTERRORISM EFFORTS
- DHS and the Federal Bureau of Investigation (FBI) continue to provide guidance to state, local, tribal and territorial partners related to the current threat environment. DHS also partners closely with the private sector to provide risk assessments and coordinate security measures with business owners and operators. The public may continue to observe law enforcement and security activity in and around public places and events.
- DHS protects the homeland from terrorism by working closely with the FBI and other intelligence partners to detect and disrupt terror suspects, putting in place additional screening and vetting measures to identify suspicious travelers and cargo, combating violent radicalization and terrorist recruitment in our communities, monitoring emerging threats, and engaging with foreign partners.
- More broadly, DHS remains committed to preventing violence and threats meant to intimidate or coerce specific populations on the basis of their religion, ethnicity or identity.

HOW YOU CAN HELP
- Report suspicious activity to local law enforcement who are best to offer specific details on terroristic indicators.
- Report suspicious activity or information about a threat, including online activity, to fusion centers and the FBI’s Field Offices - part of the Nationwide Suspicious Activity Reporting Initiative.
- Learn how to recognize signs of pre-operational planning associated with terrorism or other criminal activity.

BE PREPARED
- Be prepared for security and plan ahead. Anticipate delays and restrictions on items around populated places and at public events.
- Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs info with you.
- Connect, Plan, Train, and Report to prepare businesses & employees. Security tools/resources can be accessed through the DHS’s Hometown Security Campaign.

STAY INFORMED
- The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials.
- We urge Americans to continue to travel, attend public events, and freely associate with others but remain vigilant and aware of surroundings.
- The Department of State issues international travel alerts and warnings.
- For additional information visit Ready.
The Office of Infrastructure Protection (IP) operates the Protective Security Advisor (PSA) Program. PSAs facilitate field activities in coordination with IP divisions and other Department of Homeland Security (DHS) offices. The PSA Program maintains a robust operational field capability, conducting assessments of nationally significant critical infrastructure through Enhanced Critical Infrastructure Protection (ECIP) security surveys, Site Assistance Visits, and incident response and providing access to IP resources, training, and information.

**PSA Program**

Established in 2004, the PSA Program's primary mission is to protect critical infrastructure. The five mission areas mentioned below are carried out in direct support of this primary mission objective. Regional directors (RDs) and PSAs also conduct crosscutting information sharing and coordination activities in support of these mission areas:

- Plan, coordinate, and conduct security surveys and assessments
- Plan and conduct outreach activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Level I and II events
- Respond to incidents
- Coordinate and support improvised explosive device awareness and risk mitigation training

PSAs are security subject matter experts who engage with State, local, tribal, and territorial (SLTT) government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. They serve as regional DHS critical infrastructure security specialists, providing a local perspective to—and supporting the development of—the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical infrastructure at the regional, State, and local levels.

There are 96 RDs and PSAs, including 89 field-deployed personnel serving in 73 districts in 50 States and Puerto Rico. RDs and PSAs are strategically deployed across the United States and provide SLTT and private sector stakeholders with access to steady-state DHS risk-mitigation tools, products, and services, such as training and voluntary vulnerability assessment programs, in addition to supporting officials responsible for planning and leading NSSE and SEAR events. PSAs also support response to all-hazard incidents through field-level coordination and information sharing and provide expertise on reconstituting affected critical infrastructure. During incidents, PSAs serve as the infrastructure liaisons at the Federal Emergency Management Agency Joint Field Offices, Regional Coordination Centers, and in State and county Emergency Operations Centers. They provide expert knowledge of the affected infrastructure; maintain communications with owners and operators; and prioritize and coordinate response, recovery, and restoration efforts for critical infrastructure. Recent examples include Superstorm Sandy in 2012 and Hurricane Irene in 2011.

PSAs also conduct joint site visits and vulnerability assessments of critical infrastructure assets with the Federal Bureau of Investigation. They work with the United States Secret Service to provide vulnerability assessments, security
planning, and coordination during NSSEs and other large-scale special events, such as the Presidential Inauguration, the Super Bowl, and major international summits.

**ECIP Security Surveys**

By assessing the overall security posture of a facility, ECIP security surveys provide protective measures to critical infrastructure; inform facility owners and operators of the importance of their facilities and current terrorist threats; and develop strong relationships between critical infrastructure owners and operators, DHS, and Federal, State, and local law enforcement partners. During an ECIP visit, FSAs focus on coordination, outreach, training, and education, cataloguing existing relationships with Federal, State, local, and private sector partners. In addition, they discuss the Nationwide Suspicious Activity Reporting Initiative and the “If You See Something, Say Something”™ campaign with owners and operators.

ECIP visits are often followed by ECIP surveys to collect, process, and analyze facility assessment data and develop a detailed assessment of physical security, security management, security force, information sharing, protective measures, and dependencies to identify cascading effects. Data collected during ECIP surveys allows DHS and facility owners and operators to track the implementation of recommended protective measures, to conduct sector-by-sector and cross-sector vulnerability comparisons, to identify security gaps, to provide owners and operators with a view of their facility’s security in relation to similar facilities, and to track progress toward improving critical infrastructure security. Owners and operators are given security survey data in interactive ECIP Dashboards, which enables them to improve security postures in a cost-effective and measurable manner.

**Contact Information**

For more information, please contact PSCDOperations@hq.dhs.gov.
Homeland Security Starts with Hometown Security

The U.S. Department of Homeland Security (DHS) closely monitors attacks on public gatherings and public places to constantly enhance the Nation’s security. During both steady state and times of heightened awareness, DHS engages closely with our private sector and community partners to provide expert counsel and recommendations about protective measures they can implement to protect facilities and venues. DHS provides free tools and resources to communities because the Department recognizes that communities are the first line of defense in keeping the public safe and secure.

The Department encourages businesses to Connect, Plan, Train, and Report. Applying these four steps in advance of an incident or attack can help better prepare businesses and their employees to proactively think about the role they play in the safety and security of their businesses and communities.

CONNECT: Reach out and develop relationships in your community, including local law enforcement. Having these relationships established before an incident occurs can help speed up the response when something happens.

- Develop relationships with local law enforcement and businesses in your area. Invite local law enforcement to tour your business.
- Connect with community security and preparedness organizations such as the Federal Bureau of Investigation’s public-private partnership program “InfraGard.”
- Contact the local DHS Protective Security Advisor who is available to support your efforts.
- Communicate with your customers and let them know about the security measures you are taking to ensure a positive experience and to maintain public safety.
- If your business is located at or near a Federal facility, connect with DHS’s Federal Protective Service at 1-877-4FPS-411.

PLAN: Take the time now to plan on how you will handle a security event should one occur. Learn from other events to inform your plans.

- Be aware of current threats related to your geographic region or impacting your business sector.
- Develop plans, including security, emergency response, emergency communications, and business continuity plans, while considering the protection of your employees and customers, access control, closed-circuit television, signage, suspicious activity reporting, and parking security.
- Evaluate your security requirements and design a monitoring, surveillance, and inspection program that is consistent with your business operations.
- Develop evacuation and shelter-in-place plans, and ensure that multiple evacuation routes are clearly marked with appropriate signage and that rallying points are available.
- Develop and implement a security plan for computer and information systems hardware and software.
• Engage local first responders (police, fire, medical) in all of the above efforts to ensure your efforts are in synergy with theirs.

TRAIN: Provide your employees with training resources and exercise your plans often. The best laid plans must be exercised in order to be effective.

• Train employees on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device (IED). Ensure they understand security basics, emergency response, business continuity plans, and increased awareness of potential threats.
• Exercise your emergency communications plan.

REPORT: “If You See Something, Say Something™” is more than just a slogan. Call local law enforcement.

• Post details on reporting suspicious activity and encourage employees, tenants, and visitors to report suspicious behavior to property management security or local law enforcement. Things to consider include unattended vehicles; repeat visitors or outsiders who have no apparent business in non-public area; abandoned parcels, suitcases, backpacks, and packages; and other unusual activity.
• Get involved with the Department’s “If You See Something, Say Something™” campaign.

DHS Programs, Resources, and Tools You Can Use

Protective Security Advisors proactively engage with government partners and the private sector to protect critical infrastructure. For more information or to contact your local PSA, e-mail NICC@hq.dhs.gov.


DHS Active Shooter resources are available at http://www.dhs.gov/active-shooter-preparedness.


Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) information is available at https://nsi.ncirc.gov. SAR training for private sector partners is located at https://nsi.ncirc.gov/hspregistration/private_sector/.

Counter-Improviesm Device information and resources are available at www.dhs.gov/tripwire.

Information on DHS cybersecurity programs is available at www.dhs.gov/cyber. To find out more about the Cybersecurity Awareness Campaign, go to http://www.dhs.gov/stophinkconnect. For tips from the U.S. Computer Emergency Response Team, go to https://www.us-cert.gov/ncas/tips.

InfraGard is a public-private partnership between the FBI and the private sector that represents individuals from businesses, academic institutions, State and local law enforcement, and fire and EMS agencies, as well as other participants dedicated to sharing information, education, and intelligence. Please go to www.infragardmembers.org and https://www.infragard.org.
The Commercial Facilities (CF) Sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within this sector operate on the principle of open public access, meaning that the general public can congregate and move freely without highly visible security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities. As such, the day-to-day protection of commercial facilities is the responsibility of the owners and operators in close cooperation with local law enforcement. The potential for human and economic consequences underscore the need for the Federal Government and the CF Sector to work together to ensure the protection of these assets. The U.S. Department of Homeland Security (DHS), which serves as the CF Sector-Specific Agency (SSA), and sector partners collaboratively develop guidance, resources, and training that support the security and resilience of our Nation’s prominent business centers and gathering places.

**Commercial Facilities Sector Collaboration, Resources, and Training**

DHS offers many resources to help owners and operators manage risks, improve security, and aid the implementation and execution of protective and response measures across the CF Sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted, additional information can be found on the DHS website at [www.dhs.gov/commercial-facilities-sector](http://www.dhs.gov/commercial-facilities-sector).

**Collaboration**


Protective Security Advisors are security subject matter experts who assist local efforts to protect critical assets and provide a local perspective to the national risk picture. Learn more at [www.dhs.gov/protective-security-advisors](http://www.dhs.gov/protective-security-advisors).

Critical Infrastructure Cyber Community (CIC) Voluntary Program aligns business enterprises with existing resources to support cybersecurity risk management. Learn more at [www.dhs.gov/ccicdvp](http://www.dhs.gov/ccicdvp).

**Resources**


Suspicious activity videos and tools help owners, operators, and employees identify and report suspicious behavior and activity. Learn more at [www.dhs.gov/commercial-facilities-resources](http://www.dhs.gov/commercial-facilities-resources).

**Training**

Active shooter preparedness materials include a workshop series, online training, awareness videos, and “How To Respond” resource materials such as reference posters, guides, and cards. Learn more at [www.dhs.gov/active-shooter](http://www.dhs.gov/active-shooter).

Self-paced, no-cost online training courses on active shooter preparedness, insider threat, surveillance detection, and more are available at [www.training.fema.gov/ls/cier.aspx](http://www.training.fema.gov/ls/cier.aspx).

Webinars provide education and awareness for owners and operators on retail and hotel security, evolving threats to facilities, active shooter preparedness, and surveillance detection. Learn more at [www.dhs.gov/commercial-facilities-training](http://www.dhs.gov/commercial-facilities-training).
Sector Profile

The majority of the sector is privately owned and operated, but includes publicly traded companies and some publicly owned buildings (e.g., libraries, museums). Many facilities are considered soft targets—sites that are relatively vulnerable to a terrorist attack due to their open public access and limited security barriers. Commercial facilities are diverse in scope and function, ranging from small businesses to nationally and internationally recognized icons with large population densities when occupied. Owners and operators assess the vulnerabilities of their specific facilities and provide the funding for risk mitigation measures, making cost a significant challenge to implementing security and resilience programs.

Trends and Emerging Issues

- **Armed Attacker**: Armed attacker events at shopping centers, office buildings, and open arenas are difficult to predict or prevent, particularly given the sector’s open access design. Combating this threat requires advanced planning; resources, such as training material; and information sharing between CF subsectors and Federal, State, and local security partners.

- **Cyberattacks**: The sector widely uses the Internet for marketing, merchandising, ticketing, and reservations. A mass communications failure leading to a disruption of the Internet could affect the CF Sector as a whole and have cascading economic effects. Cyberattacks could also cause a loss of operations for automated building systems, giving hackers access to automated building systems and internal surveillance.

- **Supply Chain Disruptions**: Incredibly efficient supply chains have resulted in a “just-in-time” delivery model that leaves companies with very limited inventories, making some firms highly sensitive to supply disruptions. Supply chain disruptions could result from a range of causes, including geopolitical unrest, natural disasters, or tampered or counterfeit products.

- **Explosive Devices**: Attackers have used homemade explosives, or improvised explosive devices (IEDs), to attack commercial facilities with the aim of causing mass casualties and property damage. Open public access makes many facilities particularly vulnerable to explosives.

- **Unmanned Aircraft Systems (UAS)**: Malicious actors could use UAS or drones to gain security knowledge or private information about a facility or event in order to carry out attacks. Drones could also be used for intellectual property theft, or could be armed with a deadly weapon to execute terrorist attacks from the air.

- **Natural Disasters and Extreme Weather**: Severe weather events can cause significant property and economic damage, threaten safety of employees and guests, and restrict access to critical resources such as power, water, transportation, and food supplies.

For More Information on the Commercial Facilities Sector

- Contact the Commercial Facilities Sector-Specific Agency at cfssteam@hq.dhs.gov or learn more at www.dhs.gov/commercial-facilities-sector
Children’s Museum of Denver
at Marsico Campus
Emergency Procedure Manual

Updated 3.15.2017
EMERGENCY PROCEDURES MANUAL
THE CHILDREN’S MUSEUM

INDEX

INTRODUCTION 5

EMERGENCY PHONE NUMBERS 6
  City & County of Denver
  Denver Parks & Recreation
  Denver Water
  Elevator Company (THYSSENKRUPP)
  Elevator Phone
  Fire Protection Systems (Western States)
  Children’s Museum address & emergency phone numbers
  Police - Fire - Paramedics
  Police District 1
  Poison - Rocky Mountain Poison Center
  Public Service - Electric and Gas
  Red Cross
  United Systems – Security Alarm System

MEDICAL EMERGENCIES 7
  Assess the Situation and Act for Guests, Volunteers & Employees
  Medical Providers
  Incident Reports
  First Aid Tips
  Medical Safety Data Sheet (MSDS) location & Material Safety Data Sheet information
  Staff Certified in First Aid / CPR

HAZARDOUS WASTE AND CHEMICAL SPILLS 18
  General Information & Procedure (including PA script)
  Biological Spillage

BUILDING EVACUATION 21
  General Evacuation Guidelines
  Evacuating 3rd floor
  Evacuating 2nd floor
  Evacuating 1st floor
  Evacuating Persons with Disabilities
  Relocating Outside the Building due to Fire
  Relocating Outside the Building due to Bomb Threat
  Returning to Inside of Building
  Not Being Allowed Back Inside the Building
NOTIFYING MUSEUM ADMIN
When Administration is On-site
When Administration is Off-site
Media Relations in an Emergency

POWER OUTAGES
What to Do
What to Tell Visitors during an Outage

WATER OUTAGES
What to Do

NATURAL GAS LEAK
What to Do

FIRE
Building Evacuation
Fire Alarm versus Fire Drill
Localized Alarm
Fire Safety
Fire Evacuation Checklist

ALARMS
Alarm System, Fire Dept., Keys and Elevator Information
Localized Alarm / PA scripts
Fire Alarm Check List

WEATHER EMERGENCIES
Tornado Watches & Warnings
Tornado Procedure (including PA script)
Tornado Shelter
Severe Storm Watches & Warnings
Severe Storm/Electrical Storm Procedure (including PA script)
Lightning
Flood & Flash Flood Watches & Warnings
Flood Procedure (including PA script)
Flash Flood Procedure (including PA script)
Winter Storm/Blizzard Procedure (including PA script)
After Flooding & Weather Related Emergencies
Weather Radio

BOMB THREATS
General Information & What to Do (including PA script)
Bomb Threat Check List

ACTIVE SHOOTER 57
What to Do

ROBBERY 61
Suspect Description Form

SECURITY SYSTEM ALARM 64
Setting the Alarm
If the Alarm is Activated Accidentally
Monitoring and Notification from United Systems

BUILDING SECURITY 66
Museum Occupancy
Adults without Children
Appointments and Visitors
Teens without Adults
Lost Child
Security Cameras
Elevator Emergency Procedures
Weapons Policy

ELEVATOR EMERGENCY PROCEDURES 73
Procedures for People Trapped in the Elevator

STAFF EMERGENCY PREPAREDNESS MAINTENANCE 75
Active shooter incidents, in many cases, have no pattern or method to the selection of victims, which results in an unpredictable and evolving situation. In the midst of the chaos, anyone can play an integral role in mitigating the impacts of an active shooter incident. The Department of Homeland Security (DHS) provides a variety of no-cost resources to the public and private sector to enhance preparedness and response to an active shooter incident. The goal of the Department is to ensure awareness of actions that can be taken before, during, and after an incident.

**Active Shooter Preparedness Program**

DHS maintains a comprehensive set of resources and in-person and online trainings that focus on behavioral indicators, potential attack methods, how to develop emergency action plans, and the actions that may be taken during an incident.

**Active Shooter Online Training**

This one-hour online course (IS-907 Active Shooter: What You Can Do) provides an introductory lesson on the actions that may be taken when confronted by an active shooter, as well as indicators of workplace violence and how to manage the consequences of an incident. To access this course, please visit the Federal Emergency Management Agency (FEMA) Emergency Management Institute online training website at [http://www.training.fema.gov/is/crslist.aspx](http://www.training.fema.gov/is/crslist.aspx) and type Active Shooter in the search bar.

**Active Shooter Preparedness Workshop Series**

These scenario-based workshops feature facilitated discussions to inform participants on the best practices associated with preparing for and responding to an active shooter incident. Through a dynamic exchange of information, these workshops provide participants an understanding of how to plan and aid in the development of an initial draft of an emergency action plan for their organizations. For more information on these workshops, please contact the Active Shooter Preparedness Program at [ASworkshop@hq.dhs.gov](mailto:ASworkshop@hq.dhs.gov).

**Active Shooter Online Resources**

There are additional resources available online to inform individuals on how to prepare for active shooter incidents. These resources range from booklets and pocket guides, to a 90-minute webinar that explains the importance of developing an emergency action plan and the need to train employees on how to respond to an incident. To access these resources, please visit [http://www.dhs.gov/activeshooter](http://www.dhs.gov/activeshooter).

**Contact Information**

For general information regarding the Active Shooter Preparedness Program, please email [ASworkshop@hq.dhs.gov](mailto:ASworkshop@hq.dhs.gov).