The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Terrorism Tactics and Corresponding Protective Measures for Critical Infrastructure (Hospital Sector)

Emergency Preparedness Forum
April 7, 2017

Agenda

- Overview of the Department of Homeland Security and Critical Infrastructure;
- The Threat to Critical Infrastructure: Indicators and Protective Measures;
- Common Physical Security and Resilience Characteristics and Vulnerability and Options for Consideration for Hospitals
- The Protective Security Advisors and Resources.
Overview of the Department of Homeland Security and Critical Infrastructure

Role of DHS
- Unify a national effort to secure America
- Prevent and deter terrorist attacks
- Protect against and respond to threats and hazards to the Nation
- Respond to and recover from acts of terrorism, natural disaster, or other emergencies
- Coordinate the protection of our Nation's critical infrastructure across all sectors
Threats May Come from All Hazards

National Preparedness Goal

- Defines what it means for the whole community to be prepared for all types of disasters and emergencies
- The goal is “a more secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.”

Courtesy of DHS

Courtesy of FEMA
National Preparedness Goal (cont.)
Organizes 31 core capabilities into 5 mission areas

- **Prevention**: Prevent, avoid, or stop an imminent, threatened, or actual act of terrorism
- **Protection**: Protect our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive
- **Mitigation**: Reduce the loss of life and property by lessening the impact of future disasters
- **Response**: Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident
- **Recovery**: Recover through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident

National Response Framework

- Guides how the Nation conducts all-hazards response
- Documents the key response principles, roles, and structures that organize national response
- Allows first responders, decision-makers, and supporting entities to provide a unified national response
National Infrastructure Protection Plan (NIPP)

- Comprehensive plan and unifying structure for the public and private sector to enhance the protection and resilience of critical infrastructure
  - Partnership model
  - Risk management framework
  - Roles, responsibilities, and authorities

NIPP (cont.)

- Drives internal Department of Homeland Security (DHS) programs and activities
- Guides programs and activities for:
  - Other Federal agencies and departments
  - State, local, tribal, and territorial governments
  - Critical infrastructure owners and operators
Presidentl Policy Directive-21

- Presidential Policy Directive-21: Critical Infrastructure Security and Resilience directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

Critical Infrastructure Defined

- “Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.”

Source: National Infrastructure Protection Plan 2013
Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities

- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Protective Security Coordination Division

- Department of Homeland Security (DHS)
  - Ensures a homeland that is safe, secure, and resilient against terrorism and other hazards

- National Protection and Programs Directorate (NPPD)
  - Leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure

- Office of Infrastructure Protection (IP)
  - Leads the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community

- Protective Security Coordination Division (PSCD)
  - Provides strategic coordination and field operations support to reduce risk to the nation's critical infrastructure from a terrorist attack or natural disaster
The Threat to Critical Infrastructure: Common Indicators and Protective Measures

Trends and Tactics

- Tactics, techniques, and procedures evolve quickly and adapt to countermeasures
  - Explosives and improvised explosive devices (IEDs) can be manufactured out of common household products
  - Despite countermeasures to make explosives and IEDs difficult to conceal, adversaries remain adaptive
- Plots indicative of a common cause that rallies independent extremists to want to attack the United States
- Pre-operational indicators are becoming more and more difficult to detect, therefore State, local, and private sector partners play a critical role in identifying and reporting suspicious activity

Najibullah Zazi (Denver Post) September 25, 2009 Zazi purchasing chemicals (CNN)
The Improvised Explosive Device Threat

- IED attacks remain the primary tactic for terrorists
  - Uncomplicated
  - Inexpensive
  - Mass casualties
  - Maximum damage
- Continued global terror attacks using IEDs
  - Threat is adaptive
  - Difficult to counter

Small Unit Assaults

- Terrorists continue to use small-unit assault tactics overseas
- Small-unit attacks typically feature more advanced levels of planning, training, and preparation and may involve one or more mobile assault teams attacking a single target or several small mobile teams attacking multiple targets for extended periods
- On June 28 and 29, 2011, nine terrorists—several wearing suicide vests and carrying small arms, rocket-propelled grenades, and hand grenades—infiltrated and conducted a night attack against the Intercontinental Hotel in Kabul, Afghanistan (12 people and all nine attackers killed, 20 people wounded)
- Several small teams totaling 10 operatives used small arms, grenades, and explosives in attacks against hotels, a train station, and other public facilities in Mumbai, India on November 26-28, 2008 (166 people and 9 of 10 attackers killed)
Potential Indicators

- Employees being questioned offsite about practices pertaining to the potential target
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unusual or unannounced maintenance activities in the vicinity of the store
- Persons using or carrying video/camera/observation equipment over an extended period
- Unattended vehicles illegally parked near the buildings or places where large numbers of patrons gather

Al-Qaeda Casing Report

- Building construction vulnerabilities: Abundance of glass and its destructive power is noted throughout each of the casing reports
- Other building vulnerabilities noted:
  - Building set back
  - Location of HVAC systems
  - Substandard weight-bearing columns
  - Lack of emergency exits and escape routes
  - Inadequate sprinklers and fire detection systems
  - Focus on the physical construction of the buildings
General Protective Measures

- Planning and Preparedness
  - Develop comprehensive security and emergency response plans
  - Develop policies and procedures for dealing with hoaxes and false alarms
  - Test plans prior to an emergency to ensure preparedness
  - Post Department of Homeland Security (DHS) Bomb-making Materials Awareness Program register cards and break room posters
  - Review DHS Active Shooter training materials

- Personnel
  - Incorporate awareness and response procedures into employee training programs
  - Attend DHS Private Sector Counterterrorism Awareness Workshop

- Access Control
  - Remove any vehicles that have been parked for an unusual length of time

- Barriers
  - Install and inspect blast-resistant trash containers
  - Install active vehicle crash barriers to protect buildings and populated areas

General Protective Measures, continued

- Review procedures for facility evacuation and for shelter-in-place situations.
- Exercise procedures for dealing with emergency situations. Include staff whenever possible so that all employees have these procedures fresh in their minds.
- Invite members of LLE and Fire Agencies to participate in table top and facility exercises to increase special teams familiarity with your site and provide for best formulated response in an event.
General Protective Measures

- **Personnel**
  - Conduct background checks on all employees (more detailed checks should be conducted on those who will have access to critical assets)
  - Maintain an adequately sized, equipped, and trained security force for all events
  - Conduct continuous roving security patrols during special events; expand roving/motorized patrols to outer perimeter

- **Access Control**
  - Establish a process for controlling access to and egress from the facility; including designated, monitored points of entry
  - Establish a buffer zone and perimeter around the facility and a process for controlling access
  - Define and secure controlled areas that require extra security
General Protective Measures

- **Access Control, continued**
  - Control employee identification and access through use of photo identification badges; require badges to be displayed at all times
  - Formally identify gathering areas for tailgate parties and other such gatherings in locations with natural surveillance and access; make informal areas off-limits and subject to automatic scrutiny

- **Communication and Notification**
  - Maintain contact numbers and checklists to follow in the event of a security-related incident
  - During events, maintain instantaneous communication capability with local, state, or federal law enforcement and emergency responders
General Protective Measures

- Monitoring, Surveillance, Inspection
  - Ensure that the venue has an intrusion detection system
  - Provide video surveillance systems on venue grounds
  - At the beginning and end of each event, inspect interior/exterior of facility
  - Require screening of all patrons before they are allowed to enter the facility’s perimeter
  - Require screening of all employees, event participants, and delivery and emergency service personnel before they are allowed to enter the facility’s perimeter for special events
  - Check outdoor air intakes of heating, ventilation, and air conditioning (HVAC) systems to ensure that they are protected

- Infrastructure Interdependencies
  - Provide 24/7 guard at utility supply points starting 24 hours before a special event until its conclusion
  - Ensure that an emergency power source is provided for critical systems
  - Ensure that dumpsters are secured and enclosed
General Protective Measures

- Cyber Security
  - Minimize the number of people with authorized access to computer systems
  - Increase computer security levels to maximum practical level, if not already in place

- Incident Response
  - Ensure that multiple evacuation routes and rallying points are available
  - Inspect all available emergency equipment prior to any event to ensure that it will operate during crisis situations
  - Assign specific staff members the responsibility of turning off the gas, electricity, water, and alarm systems in the event of an emergency
Common Physical Security and Resilience Characteristics and DHS Vulnerabilities and Options for Considerations for Hospitals

Hospitals In the Past

- Very open public access
  - Numerous uncontrolled/unmonitored entries
  - Exterior doors left unlocked
- Traditionally limited security programs
  - Little or no control of visitors, contractors or vendors
  - No background checks on non-medical staff
  - Limited/no security personnel to deter or respond to threats
  - Limited emergency preparedness, security training and exercises to prepare staff
- Historically resisted becoming bastions of security
- Lacked violent crimes seen today

This Door to Remain Unlocked at all Times
Hospitals of the Present

- Despite growing threats, many hospitals still use open door policies practiced for decades
- Hospitals targeted because they are considered a soft target, the availability of drugs, and open to the public 24/7.
- Open door policy no longer practical
  - Safety requires identity and access control for everyone
  - New fire exits can prevent unauthorized hospital entry/exit undetected
- Older open design facilities much more difficult to secure

Hospital Assessment Analysis

- Between January 2009 and October 2016, nearly 340 hospitals received assessments by the U.S. Department of Homeland Security (DHS) using the Infrastructure Survey Tool (IST). Analysis of IST data identified the following physical security and general resilience characteristics among hospitals:
  - This section includes a lot of statistics, allowing our hospital audiences to compare themselves to like hospitals nationwide.
Common Physical Security and Resilience Characteristics

Security and Resilience Management

- Most hospitals have a security manager or department and an emergency manager or department. Slightly less than two-thirds of hospitals have a business continuity manager or department.
- Nearly all hospitals have an emergency action plan. Most facilities have a written security plan. Slightly more than two-thirds of facilities have a written business continuity plan.
- Nearly all hospitals conduct background checks, usually on all employees (e.g., including temporary employees). However, hospitals often do not conduct recurring background checks on employees.
- Nearly all hospitals have an incident management and command center (IMCC), almost always located onsite. Many facilities also have a backup IMCC: at nearly two-thirds of these facilities, the primary and backup IMCC are geographically separated.

Physical Security

- About two-thirds of hospitals have a high-speed avenue of approach. Facilities with this vulnerability often do not use mitigating barriers. Many facilities do not use barriers to enforce standoff distance.
- Nearly all hospitals do not use an exterior intrusion detection system (IDS). However, nearly one-half of hospitals use an interior IDS.
- Nearly all hospitals use closed-circuit television (CCTV) systems. At most hospitals, the CCTV system provides coverage that includes at least parts of the facility perimeter, areas of concern (e.g., gates, entryways), and critical areas/significant areas and assets (SAAs). Many facilities have emergency backup power for the CCTV system, and most maintain the system according to recommended specifications. Nearly all facilities record CCTV feeds, and many have a specific policy for review of recorded information.
Common Physical Security and Resilience Characteristics

**Security Force**
- Most hospitals have an onsite security force.
- Security force personnel typically do not have arrest authority, but some have detain authority.
- Security force personnel are usually unarmed and more often than not, they do not carry less-than-lethal weapons. Almost all security personnel have radios, and about one-half of facilities have security personnel who use cell phones.
- It would be very unusual for a hospital security force to lack training. Most often, security personnel participate in on-the-job training and in-house/informal training. At many facilities, they participate in formal training.
- Security personnel often have a dedicated command and control center and comprehensive post orders.

**Dependencies**
- Nearly all hospitals depend on electric power, water, wastewater removal service, communications, and information technology (IT). Most depend on critical products (e.g., chemicals), and many depend on natural gas.
- Nearly all hospitals have a diesel-fueled backup generator as an alternate that can be used in case of a loss of the primary external source of power.
- Nearly all hospitals have a manager or department responsible for IT security management. Many facilities have a cybersecurity plan. At more than two-thirds of facilities, a cybersecurity assessment has been completed.
Common Vulnerabilities and Options for Consideration

- Between October 2014 and October 2016, 65 hospitals received IST surveys that included a combined total of approximately 1,870 standard vulnerabilities and options for consideration (VOFCs).
The Protective Security Advisors and Resources
PSCD Mission Areas

- Conduct Security Surveys, Gap Analysis, and Assessments
- Conduct Outreach Activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Events
- Respond to Incidents
- Provide Improvised Explosive Device (IED) Awareness & Risk Mitigation Training

Protective Security Advisors

- PSAs are field-deployed personnel who serve as critical infrastructure security specialists
  - Regional Directors (RDs) oversee and manage the PSA program in their respective region
- State, local, tribal, and territorial (SLTT) and private sector link to DHS infrastructure protection resources
  - Coordinate vulnerability assessments, training, and other DHS products and services
  - Provide a vital link for information sharing in steady state and incident response
  - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts of the States by serving as pre-designated Infrastructure Liaisons (IL) and Deputy ILs at the Joint Field Offices
Protected Critical Infrastructure Information

- Established under the Critical Infrastructure Information Act of 2002
- Protects voluntarily submitted critical infrastructure information from:
  - Freedom of Information Act
  - State and local sunshine laws
  - Civil litigation proceedings
  - Regulatory usage
- Provides private sector with legal protections and "peace of mind."
Examples of Critical Infrastructure Information

- Protected information defined by the Critical Infrastructure Information Act includes:
  - Threats – Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of a critical asset
  - Vulnerabilities – Ability to resist threats, including assessments or estimates of vulnerability
  - Operational experience – Any past operational problem or planned or past solution including repair, recovery, or extent of incapacitation

- Any information normally available in the public domain will not be protected

Enhanced Critical Infrastructure Protection Visit

- Establishes and enhances DHS’s relationship with critical infrastructure owners and operators, informs them of the importance of their facilities, and reinforces the need for continued vigilance

- During an Enhanced Critical Infrastructure Protection (ECIP) visit, PSAs focus on coordination, outreach, training, and education

- ECIP visits are often followed by security surveys using the Infrastructure Survey Tool (IST) or Rapid Survey Tool (RST), or delivery of other IP services
Infrastructure Survey Tool

- The IST is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors
- Facilitates the consistent collection of security information
  - Physical Security
  - Security Force
  - Security Management
  - Information Sharing
  - Protective Measures
  - Dependencies

Infrastructure Survey Tool (cont.)

- Generates the Protective Measures Index and Resilience Measurement Index
- The tool allows DHS and facility owners and operators to:
  - Identify security gaps
  - Compare a facility’s security in relation to similar facilities
  - Track progress toward improving critical infrastructure security
Infrastructure Survey Tool (cont.)

- The dashboards highlight areas of potential concern and feature options to view the impact of potential enhancements to protection and resilience measures.
- The written report, developed from the IST data, contains a description of the facility and its vulnerabilities as well as recommendations to mitigate identified vulnerabilities.

IST Survey Data Categories

- Facility Information
- Contacts
- Facility Overview
- Information Sharing*
- Protective Measures Assessment*
- Criticality*
- Security Management Profile*
- Security Areas/Assets
- Additional DHS Products/Services
- Criticality Appendix
- Images
- Security Force*
- Physical Security*
  - Building Envelope
  - Delivery/Vehicle Access Control
  - Parking
  - Site's Security Force
  - Intrusion Detection System (IDS)/Close Circuit Television (CCTV)
  - Access Control
  - Security Lighting
- Cyber Vulnerability
- Dependencies*

* Comparative analysis provided
Dashboards and Information Sharing

Areas individually separated into Physical Security, Security Management, Security Force, Information Sharing, and Protective Measures. Owner/Operator can make adjustments and see improvements to individual area and overall Protective Measure Index (PMI).

Greater understanding of the most significant changes and trends.

Dashboard – Physical Security Example

Notional Information
Infrastructure Protection Gateway

**Events and Incidents Tracker** – This powerful analysis tool uses the protection and resilience data from completed surveys and assessments to enhance steady state, special event, and domestic incident support capabilities. It enables users to make decisions regarding the impact of various emergencies and to prioritize their planning, protection, response, and recovery efforts.

**Map View** – The IP Gateway’s map function enables users to drill down and view numerous data layers to specific States, counties, or cities. These layers include static layers, such as facilities-by-sector, daytime population, or street view pictures, and dynamic layers, such as current wildfire or weather elements. These geographically accurate presentations provide users with an in-depth look at an area’s operational situation.

**Digital Library** – The Digital library is a single interface through which users can access a collection of critical infrastructure resources, policy documents, and security and resilience information. This information helps users enhance critical infrastructure protection programs, prepare for and respond to incidents, and research and analyze infrastructure security and resilience data specific to their mission needs.

Infrastructure Visualization Platform

- Infrastructure Visualization Platform (IVP)
  - A data collection and presentation medium that supports critical infrastructure security, special event planning, and response operations by leveraging assessment data and other relevant materials
  - Integrates assessment data with immersive video, geospatial, and hypermedia data
  - Assists facility owners and operators, local law enforcement, and emergency response personnel to prepare for, respond to, and manage critical infrastructure, National Special Security Events (NSSEs), high-level special events, and contingency operations
In July 2010, DHS, at former Secretary Janet Napolitano’s direction, launched a national "If You See Something, Say Something™" public awareness campaign.

- The campaign was originally used by New York’s Metropolitan Transportation Authority, which licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime related efforts.
“If You See Something, Say Something™”

- The campaign is a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities.
- It underscores the critical role that the public plays in keeping our nation safe.
- DHS launched the campaign in conjunction with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

The Nationwide Suspicious Activity Reporting Initiative

- In March 2010, the Nationwide Suspicious Activity Reporting Initiative Program Management Office (PMO) was established within the U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA).
- DOJ BJA successfully nurtured the development of the NSI concept, and the initiative has matured over the past several years.
- Effective October 1, 2013, all programmatic activities performed by the NSI PMO were transitioned into the operational components of the DHS and the FBI.

The SAR process focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime. The NSI incorporates agencies’ individual SAR processes into a nationwide capability and establishes a standardized approach to processing, sharing, analyzing, and using ISE-SAR information, with the goals of detecting and preventing threats to national security, including information associated with domestic and international terrorism.
Hometown Security Partners

- The NSI has developed SAR awareness training for key non-law enforcement constituencies, or “hometown security partners,” that are important to the SAR effort.
- Educating those whose professions have a great potential of being exposed to indicators and behaviors associated with criminal and/or terrorist activity.
- Number trained since inception: over 120,000.
- Available at nsi.ncirc.gov (nsi.ncirc.gov/training_online.aspx).

“If You See Something, Say Something™”

- Only reports that document behavior reasonably indicative of criminal activity related to terrorism will be shared with Federal, State, local, tribal and territorial partners.
“If You See Something, Say Something™”

- Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious.
- For that reason, the public should report only suspicious behavior and situations (e.g., an unattended backpack in a public place or someone trying to break into a restricted area) rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity.

Partnerships

- DHS has partnered with a wide range of entities in campaign rollouts including:
  - Amtrak
  - American Hotel and Lodging Association
  - Washington Metro Area Transit Authority
  - Professional Sports Organizations (NBA, MLB, NFL)
  - Pentagon Force Protection Agency
  - Colleges and Universities
  - Individual states and cities
- DHS has translated materials into dozens of languages.
Material Pre-Requisites

- Before assisting State, local, tribal, territorial and private sector partners with drafting “If You See Something, Say Something™” materials, the DHS Office of Public Affairs (OPA) will need to obtain and verify a few items from the requestor, which are listed on the next slide.
- OPA will do all of the creative design, at no cost to partner

Material Pre-Requisites

- Required items:
  - Determine NSI compliant reporting mechanisms (must be monitored 24-7-365)
  - Provide logos to appear on materials sent in EPS vector format
  - Participate in coordination call with DHS HQ and appropriate field personnel (when necessary)
  - Optional: Offer possible images that could be included on materials
Material/Product Options

- The possibilities are endless. Be creative!

- Product Options
  - Posters, billboards, paystub inserts, tri-folds, etc.
  - Electronic materials such as Ribbon Board/Score Boards (need pixels/dimensions to design)
  - Web banners and buttons

Material/Product Options

- Placing “If You See Something, Say Something™” logo on credentials
- Public Service Announcement (PSA) – DHS can write the script for the PSA. We recommend that someone recognizable from your group record the message. DHS also has stock PSAs for use; just ask us about what we have available
- “Front/Back-of-house” materials – These will help instruct the public/employees on what to look for and what they should do in case they see something suspicious
- Materials we CANNOT create: “swag” such as pens, visors, whistles, or any other “give-away” type product
How to Contact the Campaign

- If you are interested in establishing a partnership with the “If You See Something, Say Something™” Campaign at DHS, please send your inquiries to the following address:
  - seesay@hq.dhs.gov

National Terrorism Advisory System

- The National Terrorism Advisory System (NTAS) replaces the former DHS color-coded Homeland Security Advisory System
- Regarding a potential threat, after reviewing the available information (intelligence), the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued
- NTAS Alerts will only be issued when credible information is available
National Terrorism Advisory System - Alerts

- Alert Announcements
- NTAS alerts will be issued through State, local, tribal, and territorial partners; the news media; and directly to the public via the following channels:
  - Via the official DHS NTAS webpage – [http://www.dhs.gov/alerts](http://www.dhs.gov/alerts)
  - Via email signup at – [http://www.dhs.gov/alerts](http://www.dhs.gov/alerts)
  - Via social media
    - Facebook – [http://facebook.com/NTASAlerts](http://facebook.com/NTASAlerts)
    - Twitter – [http://www.twitter.com/NTASAlerts](http://www.twitter.com/NTASAlerts)
- The public can also expect to see alerts in places, both public and private, such as transit hubs, airports, and government buildings

TRIPwire
Technical Resource for Incident Prevention

- Secure information sharing platform for IED incident information, evolving IED tactics, lessons learned, and counter-IED preparedness information
- Builds knowledge and preparedness capabilities, filling vital gaps in information sharing

Courtesy of TRIPwire
Counter-IED Training & Awareness

- Diverse curriculum of training designed to build counter-IED core capabilities, such as:
  - IED Counterterrorism Detection
  - Surveillance Detection
  - Bomb Threat Management
  - Vehicle-Borne IED (VBIED) Detection
  - Protective Measures
  - IED Search Procedures
- Increases knowledge and ability to detect, prevent, protect against, and respond to bombing threats

Counter-IED Training & Awareness

Bomb-Making Materials Awareness Program (BMAP)

- Joint DHS-FBI program that promotes private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of dual-use explosive precursor chemicals and components commonly used in IEDs
- Increases prevention opportunities by building a network of aware and vigilant private sector partners
The counter-IED capability and readiness assessment program uses a consistent, repeatable analytical methodology, field surveys, and web-accessible database for Bomb Squads, SWAT, Explosive Detection Canine Teams, and Public Safety Dive Teams.

- Increases knowledge of counter-IED capabilities at the unit, State, regional, and national-level in relation to relevant local or national preparedness goals.
- Over 1,500 units assessed since 2005.

Case Study: NCCAD Use by the State of New York (NYS)

- NYS mandated use of NCCAD in Homeland Security Grant Program justifications:
  - 2008, Bomb Squads
  - 2011, Explosive Canine Detection Teams
  - 2013, SWAT
- NYS’s NCCAD strategy addresses counter-IED capability gaps and directs investments on a State-wide basis.
- Other states are looking to NYS as a model.
MJIEDSP
Multi-Jurisdiction IED Security Planning

- A systematic process fusing counter-IED education, capability analysis, training, and planning tailored to the unique requirements of high-risk jurisdictions providing:
  - Enhanced multi-agency, multi-jurisdiction IED prevention, protection, and response capabilities
  - Integrated with National Preparedness System, including grant process and regional planning
- Over 75 workshops with after-action reports since 2007

Homeland Security Information Network (HSIN)

- HSIN (https://hsin.dhs.gov/) is DHS’s primary technology tool for trusted information sharing
- HSIN – Critical Infrastructure (HSIN-CI) enables direct communication between:
  - DHS
  - Federal, State, and local governments
  - Critical infrastructure owners and operators
- Content includes:
  - Planning and Preparedness
  - Incident Reporting and Updates
  - Situational Awareness
  - Education and Training
InfraGard

- [https://www.infragard.org](https://www.infragard.org)
- InfraGard is an information-sharing and analysis effort serving the interests of and combining the knowledge base of a wide range of members
- At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and the private sector
- InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States

Infrastructure Protection Report Series

- Increase awareness of the infrastructure mission and build a baseline of security and resilience knowledge throughout the Nation
- Identify Common Vulnerabilities, Potential Indicators of Terrorist Activity, and associated Protective Measures, along with actions that can be undertaken to enhance resilience

Courtesy of DHS
Summary

- Facilitate local field activities in coordination with other DHS offices
- Provide partners with effective vulnerability and gap analyses, bombing prevention capability analyses, and the development of protective measures to identify emerging needs and areas for investment
- Through data collection, assessment, and analysis, DHS can generate products for Federal, State, and local officials and private sector owners and operators that drive initiatives, such as infrastructure protection grant programs and research and development requirements

How Can You Help?

- Engage with PSAs and other partners on critical infrastructure protection programs and initiatives
- Encourage participation in efforts to identify, assess, and secure critical infrastructure in your community
- Communicate local concerns related to critical infrastructure protection
- Enhanced security and resilience depends on developing and strengthening partnerships between all entities with a role in critical infrastructure protection
For more information visit: www.dhs.gov/criticalinfrastructure

Chad Johnston
Protective Security Advisor-Arkansas
Chad.Johnston@hq.dhs.gov