muslim advocates
PROMOTING FREEDOM & JUSTICE FOR ALL

Improving the Safety and Security of Islamic Centers and Schools

Moderator:
Brenda F. Abdelall
Director, Program to Strengthen Charities

February 2, 2016

web: www.muslimadvocates.org
email: charities@muslimadvocates.org
phone: 202-765-4249

Introduction

- Muslim Advocates provides guidance and resources to mosques and other nonprofits.
- Many different forms of emergencies that religious institutions face:
  - Natural disasters, technological hazards, armed protests, shootings, intruders, and vandalism
- Recent threats and acts of violence against Islamic centers and schools are of particular concern.

muslim advocates
PROMOTING FREEDOM & JUSTICE FOR ALL

Agenda

- **Introductions**
- **Overview of Recent Hate Crimes and Related Investigations**
  - Madihha Ahussain, *Staff Attorney, Muslim Advocates*
- **Department of Homeland Security, Office of Infrastructure Protection**
  - Matthew Wombacher, *Current Operations Chief, Office of Infrastructure Protection, Protective Security Coordination Division*
- **Department of Education, Office of Safe and Healthy Students**
  - *Dr. Amy Banks, Center for School Preparedness*
- **Questions and Answer Session**

muslim advocates
PROMOTING FREEDOM & JUSTICE FOR ALL

For Q&A Session:

Participants can submit questions:

- **Using the webinar chat function;**
- **By e-mail to brenda@muslimadvocates.org; or**
- **By text message to 202-765-4249.**

To follow-up after the webinar, contact Muslim Advocates at charities@muslimadvocates.org or 415-692-1486

muslim advocates
PROMOTING FREEDOM & JUSTICE FOR ALL

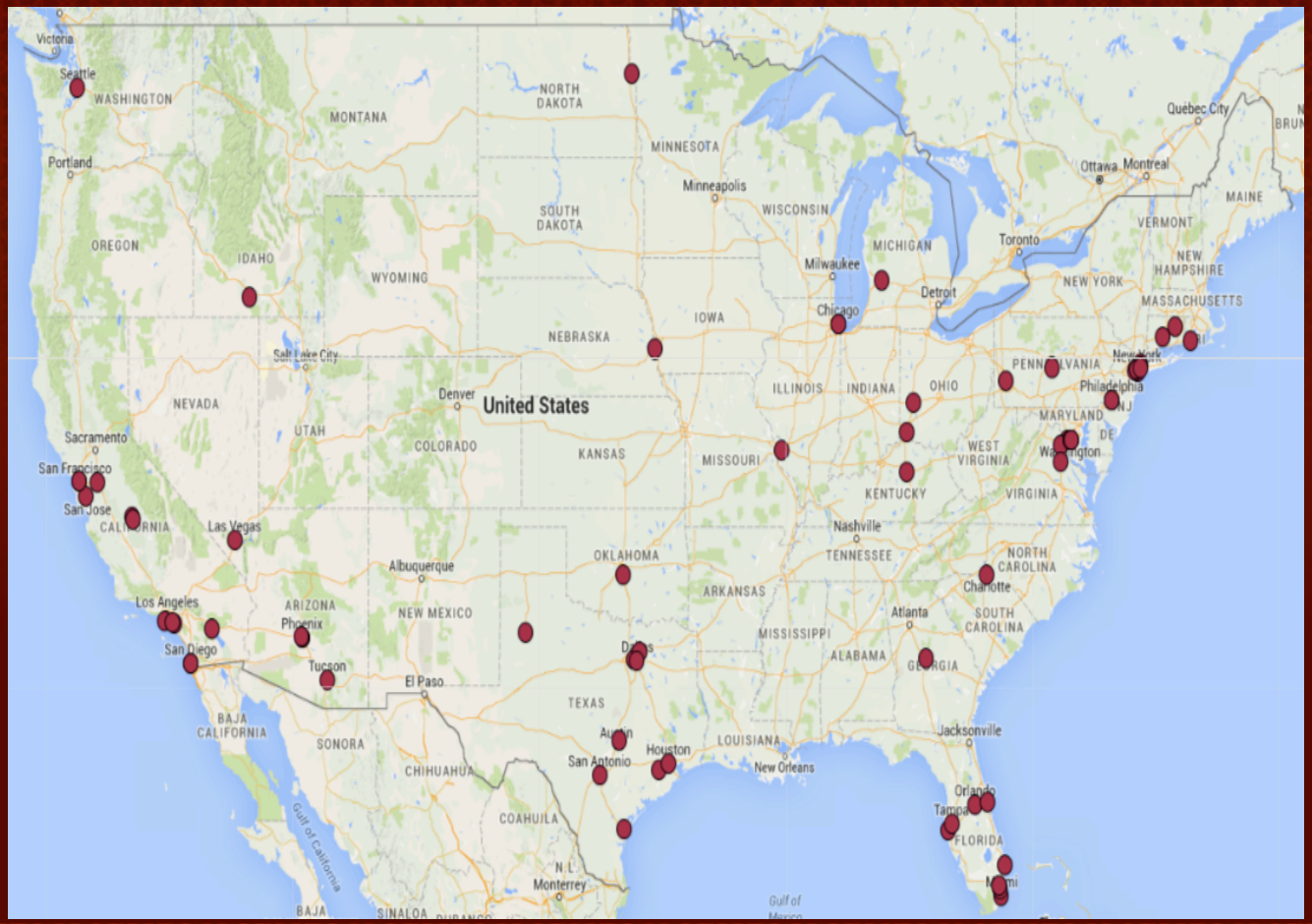
Hate Crimes in the U.S. Against American Muslims and Related Investigations

Madihha Ahussain

Staff Attorney, Muslim Advocates

madihha@muslimadvocates.org

Real Life Consequences of Bigotry



Each pin on this map represents an incident targeting Muslims or those perceived to be Muslim since the tragic November 2015 attacks in Paris.

Real Life Consequences of Bigotry

Nearly 50% involving houses of worship

Each pin on this map represents an incident targeting Muslims or those perceived to be Muslim since the tragic November 2015 attacks in Paris.

MERIDEN, CT

A man was charged with a federal hate crime offense after allegedly firing shots at the Baitul Aman Mosque.

SEMINOLE, FL

A man was charged with a federal hate crime for threatening to firebomb a mosque.

What is a hate crime?

Congress defines a hate crime as a "criminal offense against a person or property motivated in whole or in part by an offender's bias against a race, religion, disability, ethnic origin, or sexual orientation."

WHAT THE NUMBERS SAY:

FBI statistics indicate that hate crimes against Muslims continue to remain high:

- 2009: 107 reported
- ***2010: 160 reported***
- 2011: 157 reported
- 2012: 130 reported
- 2013: 135 reported
- 2014: 154 reported

Reporting Hate Crimes

According to the Department of Justice, 2 out of 3 hate crimes go unreported to the police because victims believe the police would not or could not help .

HOW TO REPORT:

- Report to *local* law enforcement **immediately**.
- Also consider reporting to:
  - Your local FBI field office
  - Your State Attorney General's office

For more information, visit:
http://www.muslimadvocates.org/reporting-hate-crimes-in-your-state/

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Religious Facilities Security and Resilience Priorities

Muslim Advocates

2016

Homeland Security

Role of Homeland Security

- 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

Courtesy of FEMA

Homeland Security

FOR OFFICIAL USE ONLY

Background

Courtesy of DHS

- The United States has approximately 345,000 religious congregations consisting of about 150 million members in 230 different denominational groups
- Religious facilities are generally open-access, public assembly venues and have been successfully targeted on numerous occasions in the past

Protective Measures Analysis

Religious Facilities

- Since 2009, PSAs have collected data on vulnerabilities and security resilience measures at about 70 religious facilities across the United States as part of the ECIP initiative
  - Potential vulnerabilities that are common across a wide spectrum of religious facilities
  - Tactics, Techniques, and Procedures commonly used to carry out attacks on public assembly areas and their relationship to religious facilities
  - Current protective measures that can effectively mitigate the threats posed by violent groups or individuals intent on attacking public assembly areas

Key Findings

Religious Facility Vulnerabilities

- Open Access
  - Unrestricted access to religious services and peripheral areas
  - Close proximity to urban areas
  - Limited or no vehicle access controls
  - Uncontrolled vendor and contractor access
  - Unprotected utilities
- Gathering of People of a Particular Faith
  - People of like faith at a single location at specified time
  - Ready target for an adversary seeking to attack that particular group
  - Facility configuration or signage can increases this vulnerability

Key Findings

Religious Facility Vulnerabilities (cont.)

- Limited Security Budget
  - Not-for-profit
  - Budgets used to pay basic operation costs and provide community services
  - Lack of financial resources to implement security measures
- Natural or Other Hazards
  - A facility's geographic location can put it in danger of specific natural hazards
  - Natural hazards can affect the safety of religious facilities and should be considered along with human threats when developing protective measures

Tactics, Techniques, and Procedures

- Tactics, Techniques, and Procedures identified in similar style attacks against public venues:
  - Attack conducted using explosive devices, small arms, grenades, knifes, hatchets
  - Attackers employed small-unit assault tactics, which involved using operatives to storm a target carrying small arms to defeat the security force
  - Attackers selected a soft target that relied on open access to the public
  - Attack designed to cause mass casualties and gain extensive media coverage.
  - Operatives wore tactical clothing and/or clothing that was not appropriate for the weather/season

Options for Consideration

- Increase “If You See Something, Say Something™” campaign awareness throughout facilities by displaying materials or providing verbal announcements
- Develop a plan for reporting suspicious activities directly to facility security and make individuals within the facility aware of the plan
- Conduct on-site visits with fire and emergency medical responders to increase their familiarity with the facility and assist in response and recovery efforts when and if needed
- If personnel capacity allows, join or institute working groups to increase information sharing among facility security personnel, law enforcement, and intelligence community partners

Options for Consideration (cont.)

- Conduct annual full-scale exercises
  - Given the unique nature of active shooter events and/or small unit assault teams, it may be beneficial to conduct full-scale exercises on a yearly basis
- Develop procedures for terrorist events, active shooters, workplace violence, and hostage situations and include them in formal security and emergency operation plans
- Increase training on hostage/barricade situations for key facility personnel, retail management, and security personnel
- Employ IDS during off-business hours, especially when security force personnel are limited
- Secure skylights or openings that could offer possible penetration points into the facility

Social Media Considerations

- Social media plays an important role in today's threat environment
  - Citizens can use social media to monitor real-time threat activity during an event
  - Law enforcement can use social media to provide critical safety instructions and awareness messages to the public

Social Media Considerations (cont.)

- Due to the restrictive nature of monitoring social media related to threat information, religious facilities should consider the following options:
  - Use social media to share safety instructions and awareness messages with your congregation
  - Monitor social media during an emergency situation or an attack to acquire critical information that could assist first responders during response and recovery operations
  - Continue information sharing activities with critical law enforcement and United States intelligence community members to ensure that accurate threat information, suspicious activities, and indicators and protective measures are shared

Key Protective Measures

- Security Management (designate security manager/develop plans)
- Resilience Management (information sharing/first responder interaction)
- Perimeter Security
- Entry Controls
- Barriers
- Electric Security Systems (Closed Circuit Television)
- Illumination
- Protect Critical Dependencies

Organizational Overview

Homeland Security

Protective Security Advisors

- Regional Directors (RDs) oversee and manage the Protective Security Advisor (PSA) program in their respective region, and PSAs are field-deployed personnel who serve as critical infrastructure security specialists
- Deployed to 73 districts in 50 States and Puerto Rico
- 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

Value of the PSA Program

- PSAs:
  - Support comprehensive risk analyses for critical infrastructure
  - Assist in the review and analysis of physical/technical security for critical infrastructure
  - Convey local concerns and sensitivities to DHS and other Federal agencies
  - Relay disconnects between local, regional, and National protection activities
  - Communicate requests for Federal training and exercises

Enhanced Critical Infrastructure Protection Visit

- Establishes/enhances DHS relationship with facility owners and operators and informs owners and operators of the importance of their facilities and the need to be vigilant
- During an ECIP visit, PSAs focus on coordination, outreach, training, and education
- Discusses the Nationwide Suspicious Activity Reporting Initiative and the "If You See Something, Say Something"™ campaign
- ECIP visits are often followed by security surveys using the Infrastructure Survey Tool (IST)

Rapid IST and Cyber IST

- Infrastructure Survey Tool (IST)
  - Demonstrated to State and local mission partners during the IP Gateway 100 person pilot to the SLTTGCC
  - IST and SAV will be available to State and local IP Gateway users
- Cyber Infrastructure Survey Tool
  - CS&C and IP collaborative initiative to deliver an integrated cyber assessment capability aligned to the IST and available on the IP Gateway
  - Developed for use by Cyber Security Advisors
- Rapid Infrastructure Survey Tool
  - Question set is a derivative of the IST and Cyber IST
  - Concise survey tool developed for State and local assessors, may also be used by the PSAs
  - Information may be used to inform the IP Gateway community of the need to conduct a full IST or Cyber IST

Infrastructure Survey Tool

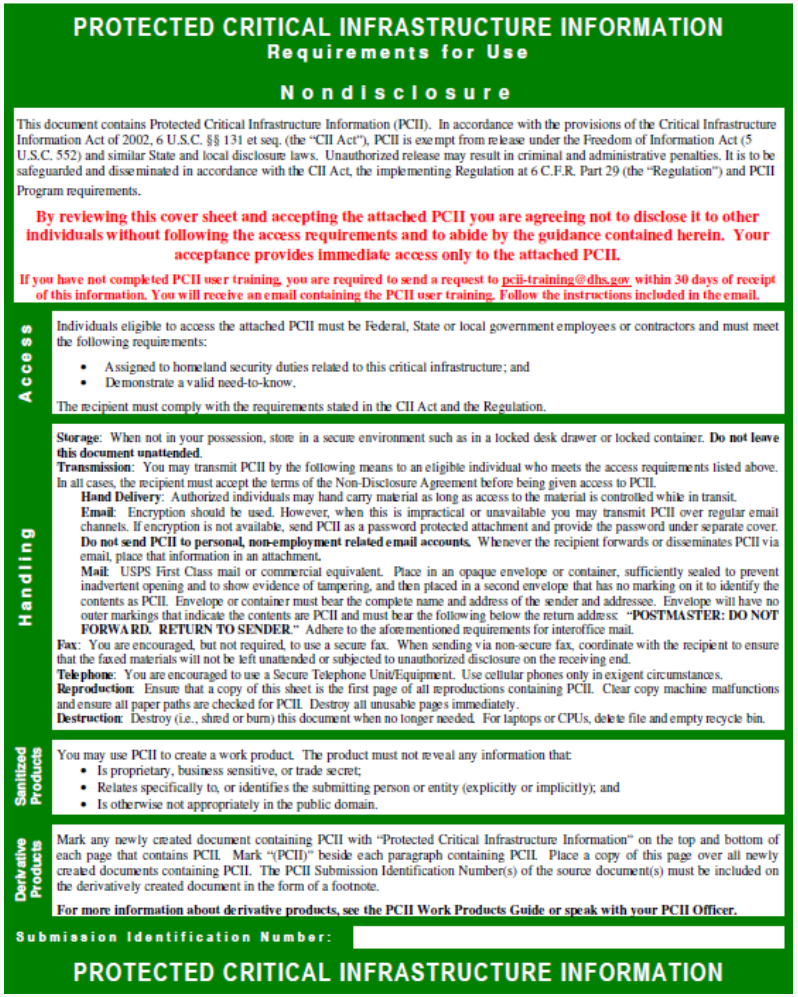
- Web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors
- Facilitates the consistent collection of security information
  - Physical Security
  - Security Force
  - Security Management
  - Information Sharing
  - Protective 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:
  - Track the implementation of recommended protective measures
  - Conduct sector-by-sector and cross-sector vulnerability comparisons
  - Identify security gaps
  - Compare a facility's security in relation to similar facilities
  - Track progress toward improving critical infrastructure security

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"



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended.**

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: **"POSTMASTER: DO NOT FORWARD. RETURN TO SENDER."** Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Courtesy of DHS

Office for Bombing Prevention

- The mission of the Office for Bombing Prevention (OBP) is to protect life and critical infrastructure by building capabilities within the general public and across the private and public sectors to prevent, protect against, respond to, and mitigate bombing incidents
- OBP accomplishes this mission through a portfolio of complementary programs:
  - Coordination of National and Intergovernmental Counter-IED Efforts
  - Information Sharing and Decision Support
  - Counter-IED Training and Awareness
  - Capability Analysis and Planning Support

Counter-IED Training and Awareness

- Diverse curriculum of training designed to build counter-IED core capabilities and enhance awareness of terrorist threats
- Increases knowledge and ability to detect, prevent, protect against, and respond to bombing threats
- Customers include State and local law enforcement and first responders, Federal agencies, and private sector partners

Counter IED Training and Awareness (cont.)

Courtesy of DHS

- Available Training and Courses:
  - VBIED Detection
  - Protective Measures
  - Surveillance Detection
  - IED Search Procedures
  - IED Counterterrorism
  - Bomb Threat Management

Homeland Security

Bomb-making Materials Awareness Program

Courtesy of DHS

- 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
- Customers include Private sector businesses and local law enforcement partners

Homeland Security

Homeland Security Information Network (HSIN)

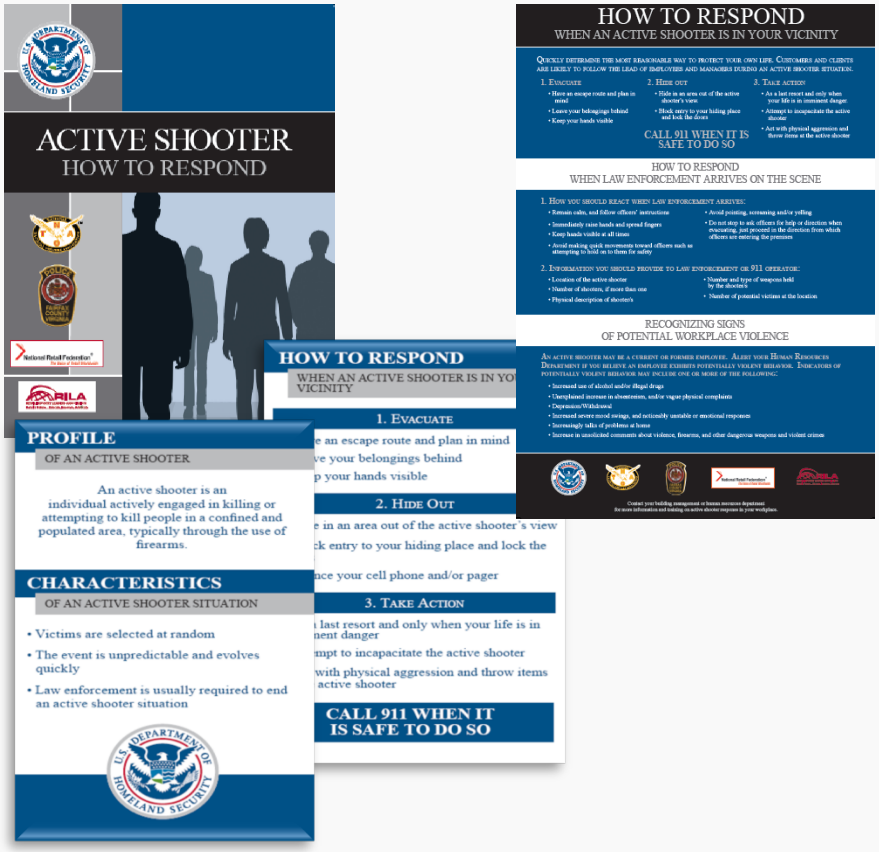
- HSIN (https://hsin.dhs.gov/) is DHS's primary technology tool for trusted information sharing
- HSIN – Critical Infrastructure (HSIN-CI) enables direct communication between:
  - DHS
  - Federal, State, and local governments
  - Critical infrastructure owners and operators

Homeland Security Information Network (cont.)

- Content includes:
  - Planning and Preparedness: Risk assessments, analysis, guidance, and security products; geospatial products and hurricane models; and exercise and national event info
  - Incident Reporting and Updates: Real-time situational reports and alerts
  - Situational Awareness: Daily and monthly sector-specific and cross-sector reports on topics ranging from cybersecurity to emerging threats
  - Education and Training: Training on topics ranging from critical infrastructure resilience, to threat detection and reaction for retail staff

Active Shooter

Training and Outreach Materials



Courtesy of DHS

- Basic Guide Book
- Pocket Emergency Measures Guide
- Break Room Poster
- To download: www.dhs.gov/activeshooter
- FEMA EMI IS907

If You See Something, Say Something ™

Courtesy of DHS

- In July 2010, DHS, at Secretary Janet Napolitano's direction, launched a national "*If You See Something, Say Something*™" public awareness campaign.
- 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

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 protection and resilience depends on developing and strengthening partnerships between all entities with a role in critical infrastructure protection

Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

Matthew R. Wombacher, CPP

Deputy Branch Chief, Field Operations

PSCDoperations@hq.dhs.gov

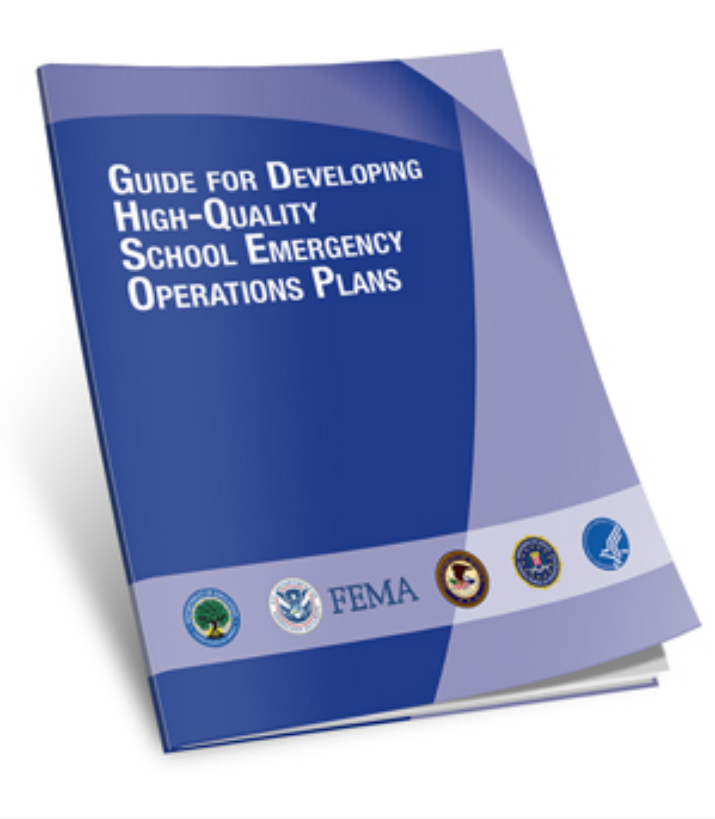
How Can You Help?

Dr. Amy Banks, Office of Safety and Healthy Students, US Department of Education

Federal Emergency Management Guidance

- Released by the White House on June 18, 2013
- First collaborative product of ED, DHS, FEMA, DOJ, FBI, and HHS

- **Available at http://rems.ed.gov:**
- Download the *Guides*
- Click through "At-a-Glance" versions
- Access supporting resources



The REMS TA Center **http://rems.ed.gov**

(855) 781-REMS [7367] info@remstacenter.org

Twitter: @remstacenter

The REMS TA Center Can Help Meet Your Emergency Management Needs

Emergency Management Needs	How the TA Center Can Help
Need help with emergency management training or professional development?	• Webinars • Online courses • TBRs
Need support developing, enhancing, or maintaining an EOP?	• EOP interactive tools • Virtual trainings
Want to connect with other practitioners or organizations ?	• The CoP can put you in touch with others who do similar work around the country
Need information on other Federal resources?	• The TA Center's comprehensive Website includes links to many resources offered by Federal partners
Need information on State requirements or resources?	• Interactive Map infographic