Homeland Security

July 10, 2018

The Office of Infrastructure Protection

National Protection and Programs Directorate Department of Homeland Security

Hometown Security

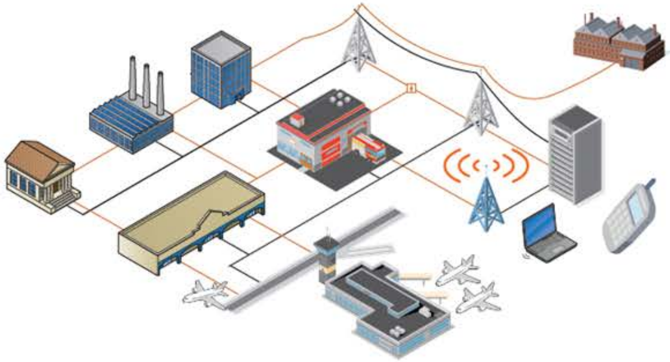
Homeland Security Starts with Hometown Security
Security starts here.
connect
plan
train
report

Homeland Security

Infrastructure Protection

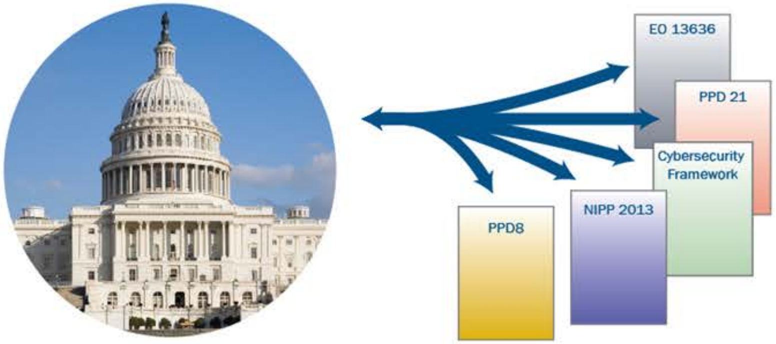
Diverse Stakeholders

Complex Interdependencies



Evolving Threats

National Policies



Whole of Community Approach

- Partnerships at all levels and shared responsibility of infrastructure security - with the types of initiatives IP has taken in an effort to enhance infrastructure security and resilience.
  - Protective Security Advisor program
  - Regional Resilience Assessment Program
  - Hometown Security
  - Active Threat Awareness - Bombing Prevention/Active Shooter
  - Chemical Security
  - Cyber Security

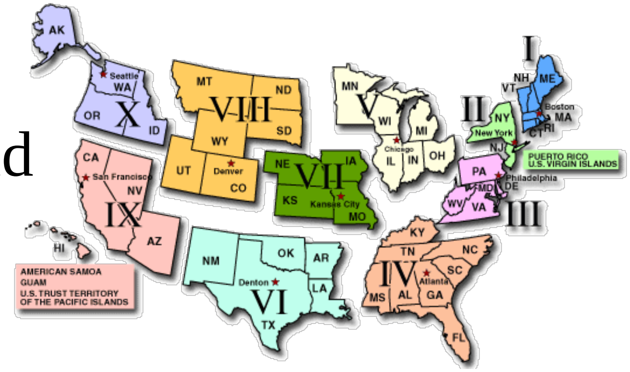
Resilient and Secure Infrastructure

- Linked to our Nation’s security and prosperity.
- CI disruption impact to national economies
- How infrastructure will be used in the coming 100 years, and how it will interact with the Internet?
- What are the threats on the horizon?

Protecting Critical Infrastructure – A Shared Responsibility

- *Challenge* continues to be copycats, lack of indicators
- *Need* balance security with open access business model
- Whole of community effort
- Partnership with owners & operators
- Recognize unique nature of operating environments
- Share information & best practices
  - SHIFT – leaning forward in how we share information
    - E.g., Paris, Brussels

Regionalization Efforts



- Strengthen coordinated delivery of IP capabilities and support to existing 300 field personnel
  - Reduce layers between mission execution and NPPD and IP leadership
  - Devolve outreach, exercises, analysis and training services, currently performed at headquarters to the regions
  - Enhance coordination regionally in steady state, special events and incident response – improving situational awareness for NPPD
- Led by a Regional Director - responsible for execution of the overall IP mission
- Assess operational needs of stakeholders and drive requirements for national IP programs and capabilities

Protective Security Advisors (PSAs)

- PSAs are field-deployed personnel who serve as critical infrastructure security specialists
  - Chief of Protective Security (CPS) 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

Hometown Security Initiative

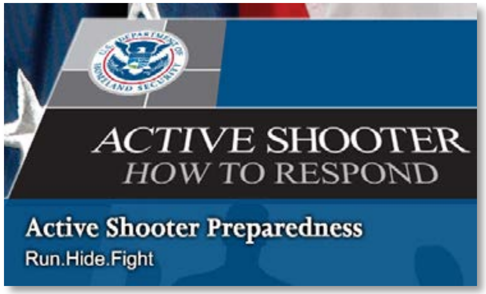
- Connect
- Plan
- Train
- Report

Website https://www.dhs.gov/hometown-security

- Active Shooter Preparedness
- Bomb Threat Training
- COOP Suite

Active Shooter Preparedness

- Plans (Active Shooter How to Respond)
- Cards, Posters, Factsheets
- Training Videos

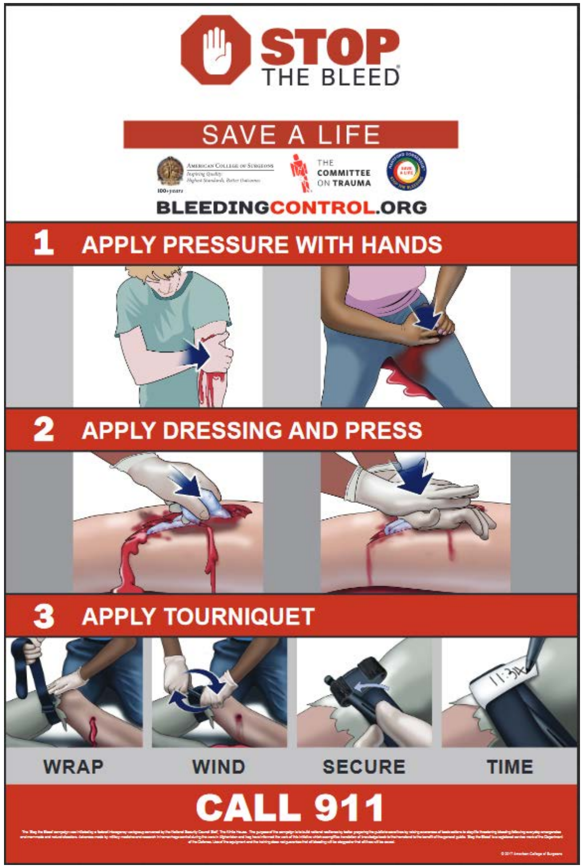


- Online Training (Active Shooter: What you can do)
- One Hour Training given by the PSA (Not Tactical)
- Active Shooter Workshops

https://www.dhs.gov/active-shooter-preparedness
https://www.govevents.com

Stop The Bleed Campaign

"Stop the Bleed" is a nationwide campaign to empower individuals to act quickly and save lives.


STOP THE BLEED

SAVE A LIFE

American College of Surgeons · THE COMMITTEE ON TRAUMA

BLEEDINGCONTROL.ORG

1 APPLY PRESSURE WITH HANDS

2 APPLY DRESSING AND PRESS

3 APPLY TOURNIQUET

WRAP WIND SECURE TIME

CALL 911

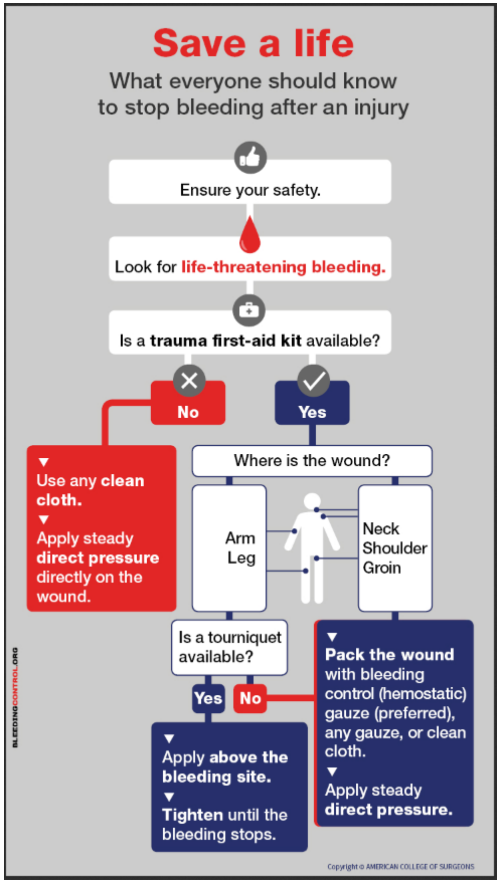
[illegible]

© 2017 American College of Surgeons

STOP THE BLEED

Website:

- ✓Free Training
- ✓Resources
- ✓Partners
- ✓Public Service Announcements


Save a life

What everyone should know to stop bleeding after an injury

Ensure your safety.

Look for **life-threatening bleeding.**

Is a **trauma first-aid kit** available?

No:
- Use any **clean cloth.**
- Apply steady **direct pressure** directly on the wound.

Yes: Where is the wound?

Arm / Leg: Is a tourniquet available?
- Yes:
  - **Apply above the bleeding site.**
  - **Tighten** until the bleeding stops.
- No: go to Neck / Shoulder / Groin

Neck / Shoulder / Groin:
- **Pack the wound** with bleeding control (hemostatic) gauze (preferred), any gauze, or clean cloth.
- Apply steady **direct pressure.**

BLEEDINGCONTROL.ORG

Copyright © AMERICAN COLLEGE OF SURGEONS

https://www.bleedingcontrol.org/

U.S. DEPARTMENT OF HOMELAND SECURITY Homeland Security

National SAR Initiative

- Joint effort between DHS, FBI, State, Local, Tribal, and Territorial law enforcement partners
- Online Training with certificate
  - What is Suspicious Activity, Items, how to report, etc.
- Resources

NSI
Suspicious Activity Reporting
Private Sector Security Training
Private Sector Security

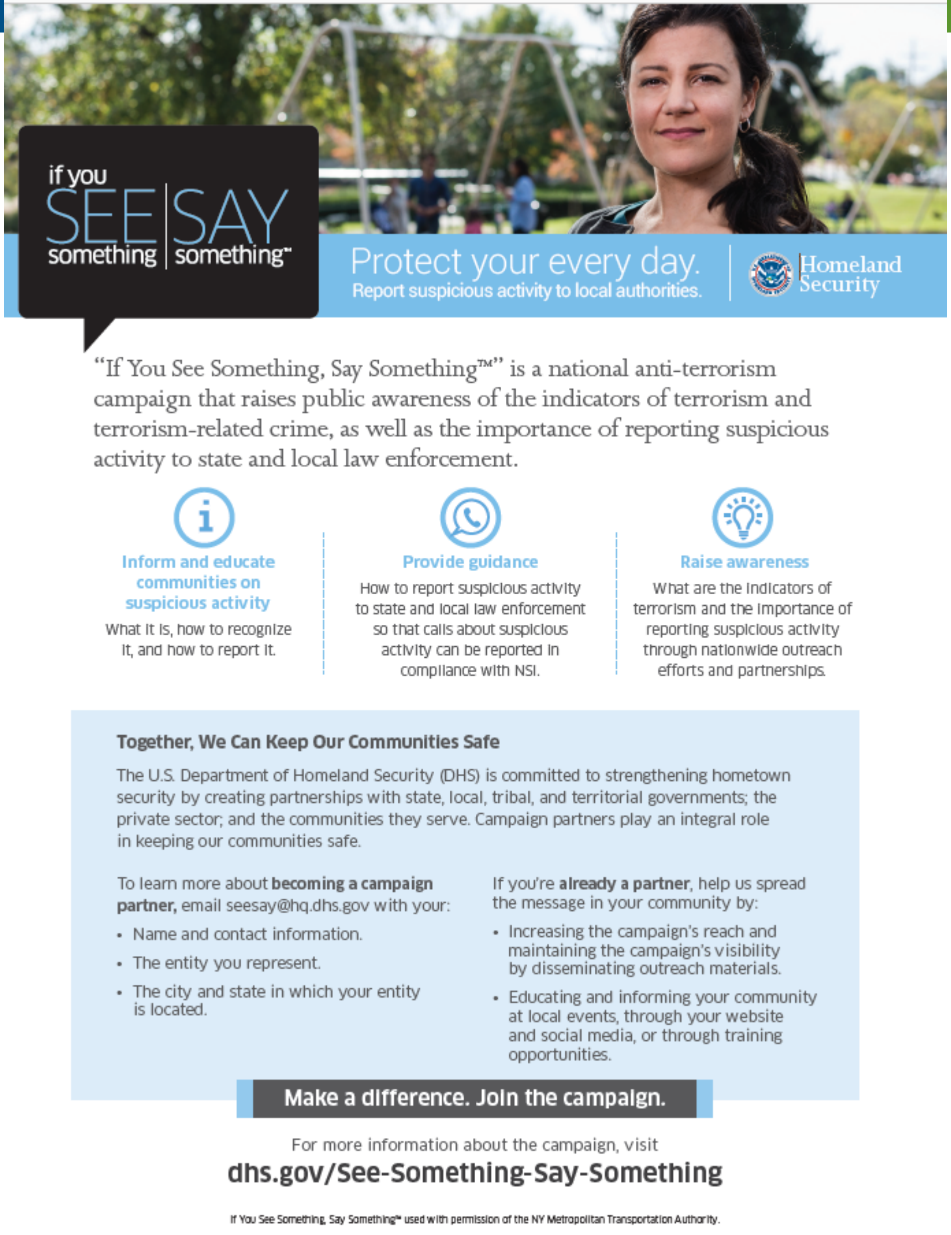
https://nsi.ncirc.gov/

DHS See Something, Say Something

If you see something, say something
What is Suspicious Activity?
About the Campaign
Become a Partner
Campaign Materials
Take the Challenge!
DO YOU KNOW
HOW TO REPORT SUSPICIOUS ACTIVITY?
LEARN HOW
If you see something, say something

https://www.dhs.gov/see-something-say-something

Homeland Security



if you SEE | SAY something | something™

Protect your every day.
Report suspicious activity to local authorities.

Homeland Security

"If You See Something, Say Something™" is a national anti-terrorism campaign that raises public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law enforcement.

Inform and educate communities on suspicious activity
What it is, how to recognize it, and how to report it.

Provide guidance
How to report suspicious activity to state and local law enforcement so that calls about suspicious activity can be reported in compliance with NSI.

Raise awareness
What are the indicators of terrorism and the importance of reporting suspicious activity through nationwide outreach efforts and partnerships.

Together, We Can Keep Our Communities Safe

The U.S. Department of Homeland Security (DHS) is committed to strengthening hometown security by creating partnerships with state, local, tribal, and territorial governments; the private sector; and the communities they serve. Campaign partners play an integral role in keeping our communities safe.

To learn more about **becoming a campaign partner,** email seesay@hq.dhs.gov with your:

- Name and contact information.
- The entity you represent.
- The city and state in which your entity is located.

If you're **already a partner**, help us spread the message in your community by:

- Increasing the campaign's reach and maintaining the campaign's visibility by disseminating outreach materials.
- Educating and informing your community at local events, through your website and social media, or through training opportunities.

Make a difference. Join the campaign.

For more information about the campaign, visit
dhs.gov/See-Something-Say-Something

If You See Something, Say Something™ used with permission of the NY Metropolitan Transportation Authority.

Homeland Security Information Network (HSIN)

- https://hsin.dhs.gov/
- HSIN 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

Cybersecurity Advisory Program

Mission:

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation’s Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

Priorities:

- Protection & Sustainment of Critical Infrastructure
- Information Sharing
- Incident Response Support

DHS Cyber Security Tools / Resources

Cyber Security Assessments:

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Phishing Campaign Assessment (PCA)
- Risk & Vulnerability Assessment (RVA) | Pen Test
- Cyber Hygiene (CH) | Vulnerability Scanning
- Industrial Control Systems (ICS) Survey

Information Sharing and Threat Analysis:

- Automated Indicator Sharing | Threat Feed
- Cyber Information Sharing & Collaboration Program (CISCP) | Trusted Circle
- Enhanced Cybersecurity Service (ECS) | Intrusion Prevention

Incident Reporting/Response:

- Proactive Hunt & Incident Response Team

Homeland Security

Cyber Security Evaluation Tool

- Self Assessment
- Select Standards
- Determine Assurance Level
- Create Diagram
- Answer the Questions
- Review Analysis and Reports
- Get started by downloading CSET at https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

CSET®
CYBER SECURITY EVALUATION TOOL
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
Homeland Security

Incident Reporting/Malware Analysis

24x7 contact number: 1-888-282-0870

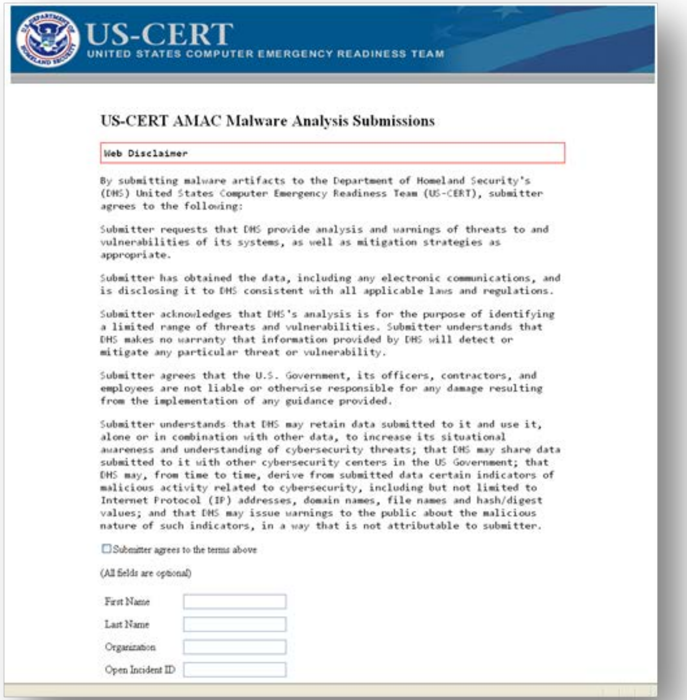
When to Report:

If there is a suspected or confirmed cyber attack or incident that:

- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

Advanced Malware Analysis Center:

- Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.
- Must be provided in password-protected zip files using password “infected”
- Email Submission: submit@malware.us-cert.gov
- Web Submission: https://malware.us-cert.gov



US-CERT AMAC Malware Analysis Submissions

Web Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

☐ Submitter agrees to the terms above

(All fields are optional)

First Name

Last Name

Organization

Open Incident ID

Homeland
Security

DHS Contact Information

George W. Reeves

Cyber Security Advisor

Office of Cybersecurity &
Communications

U.S. Department of Homeland Security
Greater Houston, Austin & San Antonio
Regions

Email: george.reeves@hq.dhs.gov
Mobile: (281) 714-1259

Stop. Think. Connect.

- Join The Campaign
- Campaign Blog
- Promotional Materials
- Toolkit
- Videos

STOP | THINK
CONNECT™

https://www.dhs.gov/stopthinkconnect

Bombing Prevention

- The Office for Bombing Prevention (OBP) mission 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 Bombing Prevention Efforts
  - Information Sharing and Decision Support
  - Counter-IED Training and Awareness
  - Capability Analysis and Planning Support

Counter-IED Training & Awareness

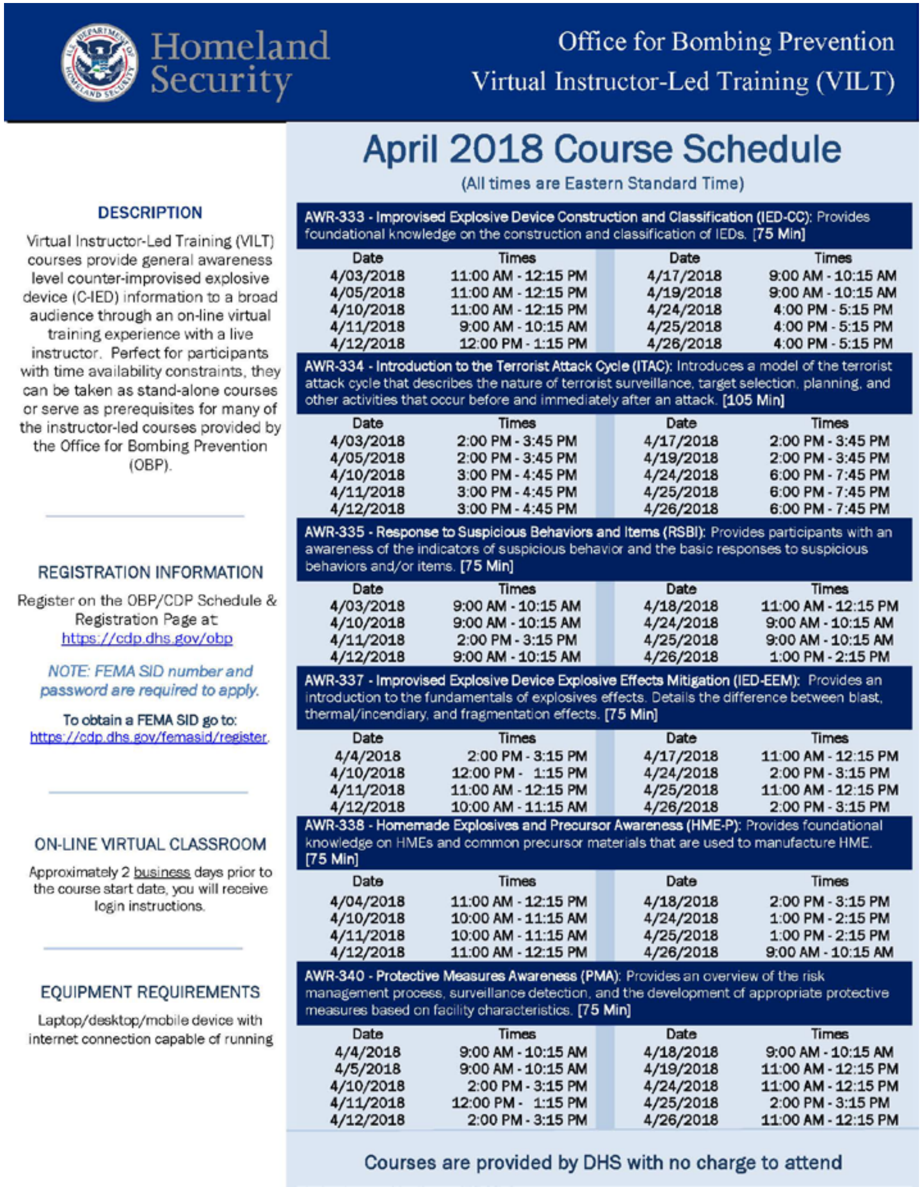
Courtesy of DHS OBP

- 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

OBP VILT

- Live Instructor
- FEMA SID
- Registration
- HSIN Connect
- Free of charge
- Anyone can take these classes

Website:
https://cdp.dhs.gov/obp



Homeland Security

Office for Bombing Prevention
Virtual Instructor-Led Training (VILT)

April 2018 Course Schedule

(All times are Eastern Standard Time)

DESCRIPTION

Virtual Instructor-Led Training (VILT) courses provide general awareness level counter-improvised explosive device (C-IED) information to a broad audience through an on-line virtual training experience with a live instructor. Perfect for participants with time availability constraints, they can be taken as stand-alone courses or serve as prerequisites for many of the instructor-led courses provided by the Office for Bombing Prevention (OBP).

REGISTRATION INFORMATION

Register on the OBP/CDP Schedule & Registration Page at https://cdp.dhs.gov/obp

NOTE: FEMA SID number and password are required to apply.

To obtain a FEMA SID go to: https://cdp.dhs.gov/femasid/register.

ON-LINE VIRTUAL CLASSROOM

Approximately 2 business days prior to the course start date, you will receive login instructions.

EQUIPMENT REQUIREMENTS

Laptop/desktop/mobile device with internet connection capable of running

AWR-333 - Improvised Explosive Device Construction and Classification (IED-CC): Provides foundational knowledge on the construction and classification of IEDs. **[75 Min]**

Date	Times	Date	Times
4/03/2018	11:00 AM - 12:15 PM	4/17/2018	9:00 AM - 10:15 AM
4/05/2018	11:00 AM - 12:15 PM	4/19/2018	9:00 AM - 10:15 AM
4/10/2018	11:00 AM - 12:15 PM	4/24/2018	4:00 PM - 5:15 PM
4/11/2018	9:00 AM - 10:15 AM	4/25/2018	4:00 PM - 5:15 PM
4/12/2018	12:00 PM - 1:15 PM	4/26/2018	4:00 PM - 5:15 PM

AWR-334 - Introduction to the Terrorist Attack Cycle (ITAC): Introduces a model of the terrorist attack cycle that describes the nature of terrorist surveillance, target selection, planning, and other activities that occur before and immediately after an attack. **[105 Min]**

Date	Times	Date	Times
4/03/2018	2:00 PM - 3:45 PM	4/17/2018	2:00 PM - 3:45 PM
4/05/2018	2:00 PM - 3:45 PM	4/19/2018	2:00 PM - 3:45 PM
4/10/2018	3:00 PM - 4:45 PM	4/24/2018	6:00 PM - 7:45 PM
4/11/2018	3:00 PM - 4:45 PM	4/25/2018	6:00 PM - 7:45 PM
4/12/2018	3:00 PM - 4:45 PM	4/26/2018	6:00 PM - 7:45 PM

AWR-335 - Response to Suspicious Behaviors and Items (RSBI): Provides participants with an awareness of the indicators of suspicious behavior and the basic responses to suspicious behaviors and/or items. **[75 Min]**

Date	Times	Date	Times
4/03/2018	9:00 AM - 10:15 AM	4/18/2018	11:00 AM - 12:15 PM
4/10/2018	9:00 AM - 10:15 AM	4/24/2018	9:00 AM - 10:15 AM
4/11/2018	2:00 PM - 3:15 PM	4/25/2018	9:00 AM - 10:15 AM
4/12/2018	9:00 AM - 10:15 AM	4/26/2018	1:00 PM - 2:15 PM

AWR-337 - Improvised Explosive Device Explosive Effects Mitigation (IED-EEM): Provides an introduction to the fundamentals of explosives effects. Details the difference between blast, thermal/incendiary, and fragmentation effects. **[75 Min]**

Date	Times	Date	Times
4/4/2018	2:00 PM - 3:15 PM	4/17/2018	11:00 AM - 12:15 PM
4/10/2018	12:00 PM - 1:15 PM	4/24/2018	2:00 PM - 3:15 PM
4/11/2018	11:00 AM - 12:15 PM	4/25/2018	11:00 AM - 12:15 PM
4/12/2018	10:00 AM - 11:15 AM	4/26/2018	2:00 PM - 3:15 PM

AWR-338 - Homemade Explosives and Precursor Awareness (HME-P): Provides foundational knowledge on HMEs and common precursor materials that are used to manufacture HME. **[75 Min]**

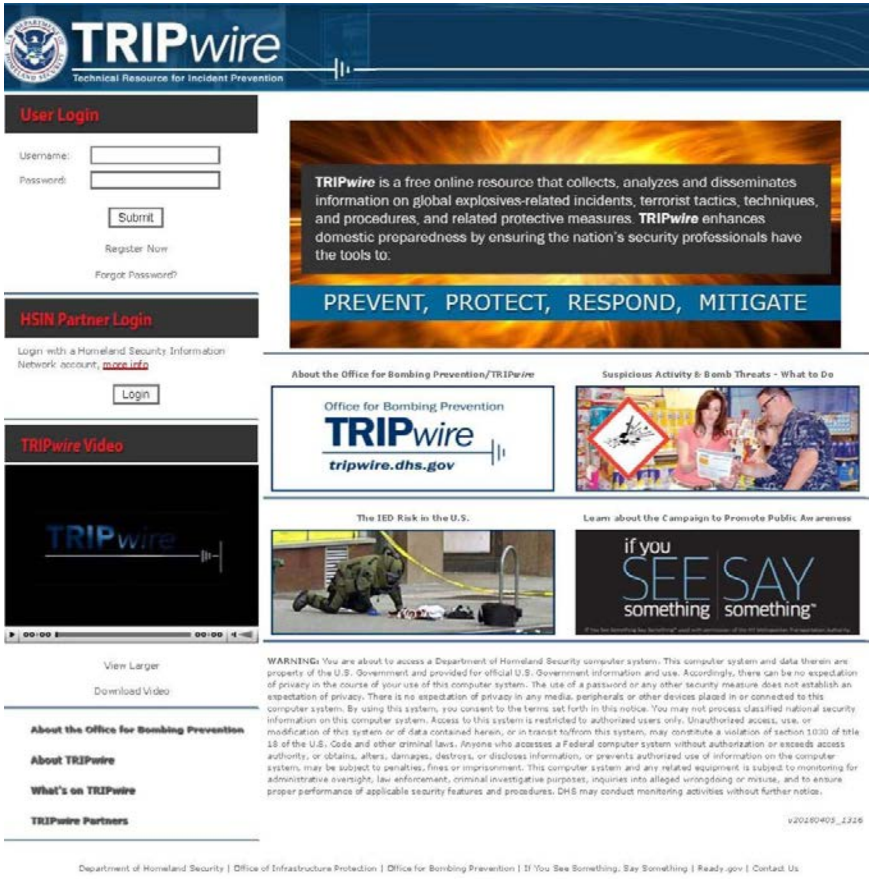
Date	Times	Date	Times
4/04/2018	11:00 AM - 12:15 PM	4/18/2018	2:00 PM - 3:15 PM
4/10/2018	10:00 AM - 11:15 AM	4/24/2018	1:00 PM - 2:15 PM
4/11/2018	10:00 AM - 11:15 AM	4/25/2018	1:00 PM - 2:15 PM
4/12/2018	11:00 AM - 12:15 PM	4/26/2018	9:00 AM - 10:15 AM

AWR-340 - Protective Measures Awareness (PMA): Provides an overview of the risk management process, surveillance detection, and the development of appropriate protective measures based on facility characteristics. **[75 Min]**

Date	Times	Date	Times
4/4/2018	9:00 AM - 10:15 AM	4/18/2018	9:00 AM - 10:15 AM
4/5/2018	9:00 AM - 10:15 AM	4/19/2018	11:00 AM - 12:15 PM
4/10/2018	2:00 PM - 3:15 PM	4/24/2018	11:00 AM - 12:15 PM
4/11/2018	12:00 PM - 1:15 PM	4/25/2018	2:00 PM - 3:15 PM
4/12/2018	2:00 PM - 3:15 PM	4/26/2018	11:00 AM - 12:15 PM

Courses are provided by DHS with no charge to attend

TRIPwire



TRIPwire

Technical Resource for Incident Prevention

User Login

Username:

Password:

HSIN Partner Login

Login with a Homeland Security Information Network account, more info

TRIPwire Video

About the Office for Bombing Prevention

About TRIPwire

What's on TRIPwire

TRIPwire Partners

TRIPwire is a free online resource that collects, analyzes and disseminates information on global explosives-related incidents, terrorist tactics, techniques, and procedures, and related protective measures. **TRIPwire** enhances domestic preparedness by ensuring the nation's security professionals have the tools to:

PREVENT, PROTECT, RESPOND, MITIGATE

About the Office for Bombing Prevention/TRIPwire

Suspicious Activity & Bomb Threats - What to Do

The IED Risk in the U.S.

Learn about the Campaign to Promote Public Awareness

WARNING: You are about to access a Department of Homeland Security computer system. This computer system and data therein are property of the U.S. Government and provided for official U.S. Government information and use. Accordingly, there can be no expectation of privacy in the course of your use of this computer system. The use of a password or any other security measure does not establish an expectation of privacy. There is no expectation of privacy in any media, peripherals or other devices placed in or connected to this computer system. By using this system, you consent to the terms set forth in this notice. You may not process classified national security information on this computer system. Access to this system is restricted to authorized users only. Unauthorized access, use, or modification of this system or of data contained herein, or in transit to/from this system, may constitute a violation of section 1030 of title 18 of the U.S. Code and other criminal laws. Anyone who accesses a Federal computer system without authorization or exceeds access authority, or obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer system, may be subject to penalties, fines or imprisonment. This computer system and any related equipment is subject to monitoring for administrative oversight, law enforcement, criminal investigative purposes, inquiries into alleged wrongdoing or misuse, and to ensure proper performance of applicable security features and procedures. DHS may conduct monitoring activities without further notice.

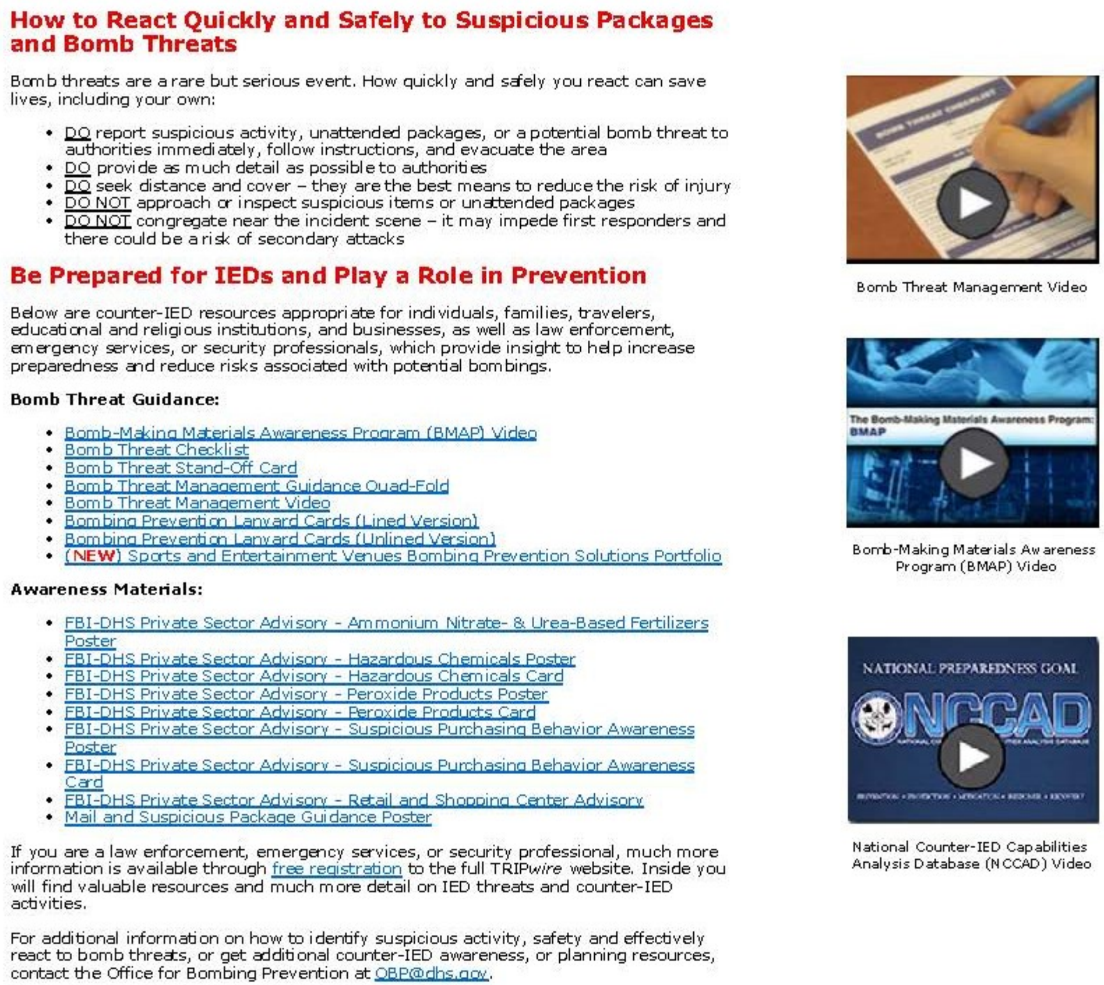
v20180405_1326

Department of Homeland Security | Office of Infrastructure Protection | Office for Bombing Prevention | If You See Something, Say Something | Ready.gov | Contact Us

Courtesy of TRIPwire

- 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

TRIPwire



How to React Quickly and Safely to Suspicious Packages and Bomb Threats

Bomb threats are a rare but serious event. How quickly and safely you react can save lives, including your own:

- DO report suspicious activity, unattended packages, or a potential bomb threat to authorities immediately, follow instructions, and evacuate the area
- DO provide as much detail as possible to authorities
- DO seek distance and cover – they are the best means to reduce the risk of injury
- DO NOT approach or inspect suspicious items or unattended packages
- DO NOT congregate near the incident scene – it may impede first responders and there could be a risk of secondary attacks

Be Prepared for IEDs and Play a Role in Prevention

Below are counter-IED resources appropriate for individuals, families, travelers, educational and religious institutions, and businesses, as well as law enforcement, emergency services, or security professionals, which provide insight to help increase preparedness and reduce risks associated with potential bombings.

Bomb Threat Guidance:

- Bomb-Making Materials Awareness Program (BMAP) Video
- Bomb Threat Checklist
- Bomb Threat Stand-Off Card
- Bomb Threat Management Guidance Quad-Fold
- Bomb Threat Management Video
- Bombing Prevention Lanyard Cards (Lined Version)
- Bombing Prevention Lanyard Cards (Unlined Version)
- (NEW) Sports and Entertainment Venues Bombing Prevention Solutions Portfolio

Awareness Materials:

- FBI-DHS Private Sector Advisory - Ammonium Nitrate- & Urea-Based Fertilizers Poster
- FBI-DHS Private Sector Advisory - Hazardous Chemicals Poster
- FBI-DHS Private Sector Advisory - Hazardous Chemicals Card
- FBI-DHS Private Sector Advisory - Peroxide Products Poster
- FBI-DHS Private Sector Advisory - Peroxide Products Card
- FBI-DHS Private Sector Advisory - Suspicious Purchasing Behavior Awareness Poster
- FBI-DHS Private Sector Advisory - Suspicious Purchasing Behavior Awareness Card
- FBI-DHS Private Sector Advisory - Retail and Shopping Center Advisory
- Mail and Suspicious Package Guidance Poster

If you are a law enforcement, emergency services, or security professional, much more information is available through free registration to the full TRIP*wire* website. Inside you will find valuable resources and much more detail on IED threats and counter-IED activities.

For additional information on how to identify suspicious activity, safety and effectively react to bomb threats, or get additional counter-IED awareness, or planning resources, contact the Office for Bombing Prevention at OBP@dhs.gov.

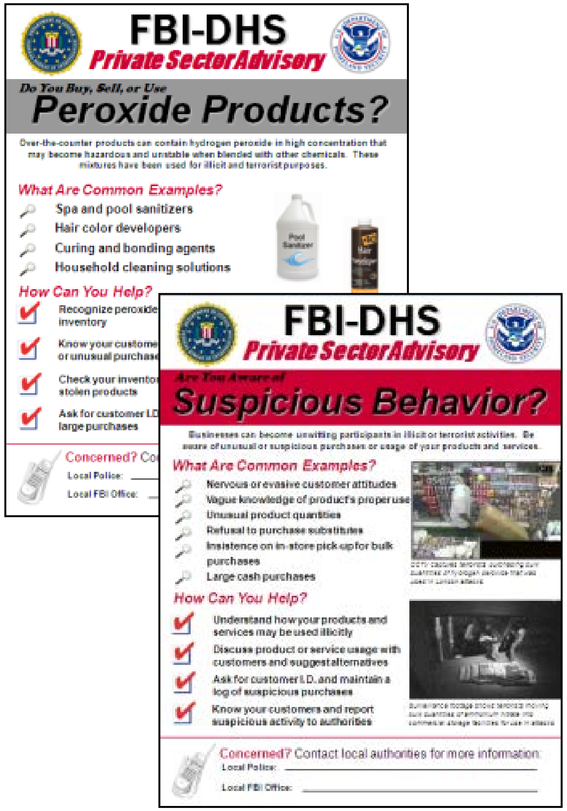
Bomb Threat Management Video

Bomb-Making Materials Awareness Program (BMAP) Video

National Counter-IED Capabilities Analysis Database (NCCAD) Video

- Bomb threat guidance materials available for download
- Awareness materials

Counter-IED Training & Awareness



FBI-DHS
Private Sector Advisory

Do You Buy, Sell, or Use
Peroxide Products?

Over-the-counter products can contain hydrogen peroxide in high concentration that may become hazardous and unstable when blended with other chemicals. These mixtures have been used for illicit and terrorist purposes.

What Are Common Examples?

- Spa and pool sanitizers
- Hair color developers
- Curing and bonding agents
- Household cleaning solutions

How Can You Help?

- ✓ Recognize peroxide inventory
- ✓ Know your custome or unusual purchase
- ✓ Check your invento stolen products
- ✓ Ask for customer I.D large purchases

Concerned? Co
Local Police:
Local FBI Office:

FBI-DHS
Private Sector Advisory

Are You Aware of
Suspicious Behavior?

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

What Are Common Examples?

- Nervous or evasive customer attitudes
- Vague knowledge of product's proper use
- Unusual product quantities
- Refusal to purchase substitutes
- Insistence on in-store pick-up for bulk purchases
- Large cash purchases

CCTV captures terrorists purchasing bulk quantities of hydrogen peroxide that was used in London attacks

How Can You Help?

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

Surveillance footage shows terrorists moving bulk quantities of ammonium nitrate into commercial storage facilities for use in attacks

Concerned? Contact local authorities for more information:
Local Police: ______
Local FBI Office: ______

Courtesy of DHS/FBI

- 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

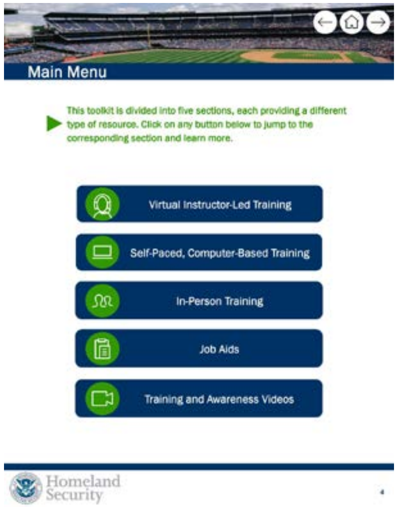
Other Products and Services

Department of Homeland Security
Office for Bombing Prevention

Sports and Entertainment Venues
Bombing Prevention Solutions Portfolio

Homeland Security

Ready, Set, Start!


Main Menu

This toolkit is divided into five sections, each providing a different type of resource. Click on any button below to jump to the corresponding section and learn more.

Virtual Instructor-Led Training

Self-Paced, Computer-Based Training

In-Person Training

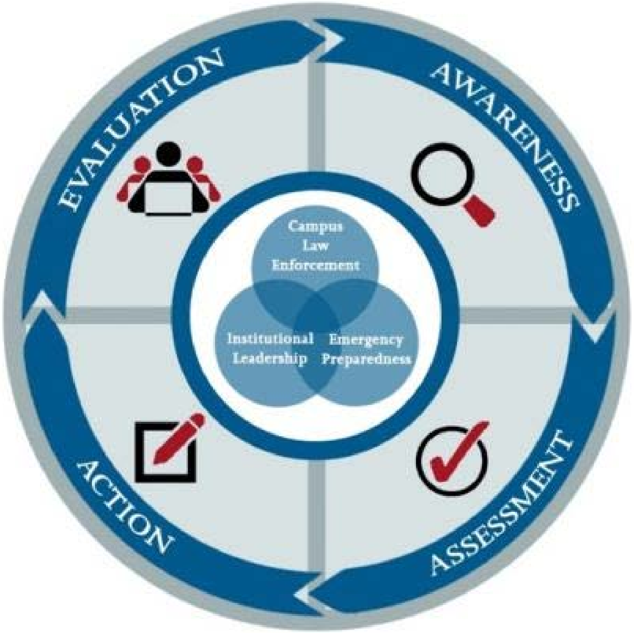
Job Aids

Training and Awareness Videos

Homeland Security

- Bombing Prevention Solutions Portfolio
- One-stop shop for countering the threat of explosives
- Toolkit divided into five sections
  - VILT
  - Self-Paced, Computer-Based
  - In-Person Training
  - Job Aids
  - Training and Awareness Videos

Other Products and Services



- Campus Resilience Program Resource Library
- Online repository of resources to empower campus leaders to enhance security and resilience
- Resources organized according to specific threat/hazard
- Further categorized according to its relevant Mission Area
- https://www.dhs.gov/campus-resilience-program-resource-library

InfraGard

- 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

The Chemical Facility Anti-Terrorism Standards

- DHS regulates security at high-risk chemical facilities through the CFATS program
- CFATS follows a risk-based approach, allowing DHS to focus on high-risk chemical facilities

– To determine if a facility is subject to CFATS, DHS looks at the unique circumstances faced by the facility

  – If the facility is in possession of threshold quantities of Appendix A Chemicals of Interest (COI), the facility must provide information to the Department to support risk assessment
  – This applies even if the facility does not consider itself a “chemical facility”—CFATS applies to hospitals, mines, universities, etc.

Available Resources

Outreach: DHS outreach for CFATS is a continuous effort to educate stakeholders on the program.

- To request a CFATS presentation or a CAV, individuals may submit a request through the program Web site, located at www.dhs.gov/chemicalsecurity, or by e-mailing DHS at CFATS@dhs.gov.

CFATS Help Desk: DHS has developed a CFATS Help Desk that individuals can call or email with questions on the CFATS program.

- Hours of Operation are 8:30 AM – 5:00 PM (ET), Monday through Friday
- The CFATS Help Desk toll-free number is 1-866-323-2957
- The CFATS Help Desk email address is csat@dhs.gov

CFATS Web Site: For CFATS Frequently Asked Questions (FAQs), CVI training, and other useful CFATS-related information, please go to www.dhs.gov/chemicalsecurity.

Questions

Homeland Security

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

CF “Buck” Hamilton, PSA – West Texas
cf.hamilton@dhs.gov

Lee Otten, PSA
Edwin.otten@dhs.gov

Bryan Gray, PSA
Bryan.Gray@hq.dhs.gov

Jeff Murray, PSA
Jeffrey.Murray@hq.dhs.gov

Rick Cary, PSA
richard.cary@HQ.DHS.GOV