U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

"DEFEND TODAY,
SECURE TOMORROW."

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Infrastructure Security Division

Infrastructure Security Division leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

MISSION PRIORITIES:

- Secure critical infrastructure from terrorist attacks.
- Work with government and private sector partners to increase security around soft targets and crowded places through training, exercises, assessments and other resources
- Collaborate with government partners to share security best practices, conduct assessments and share information related to school safety
- Prevent complex or hybrid attacks in a converging cyber-physical threat landscape
- Manage regulatory compliance of securing chemical facilities through the Chemical Facility Anti-Terrorism Standards program.

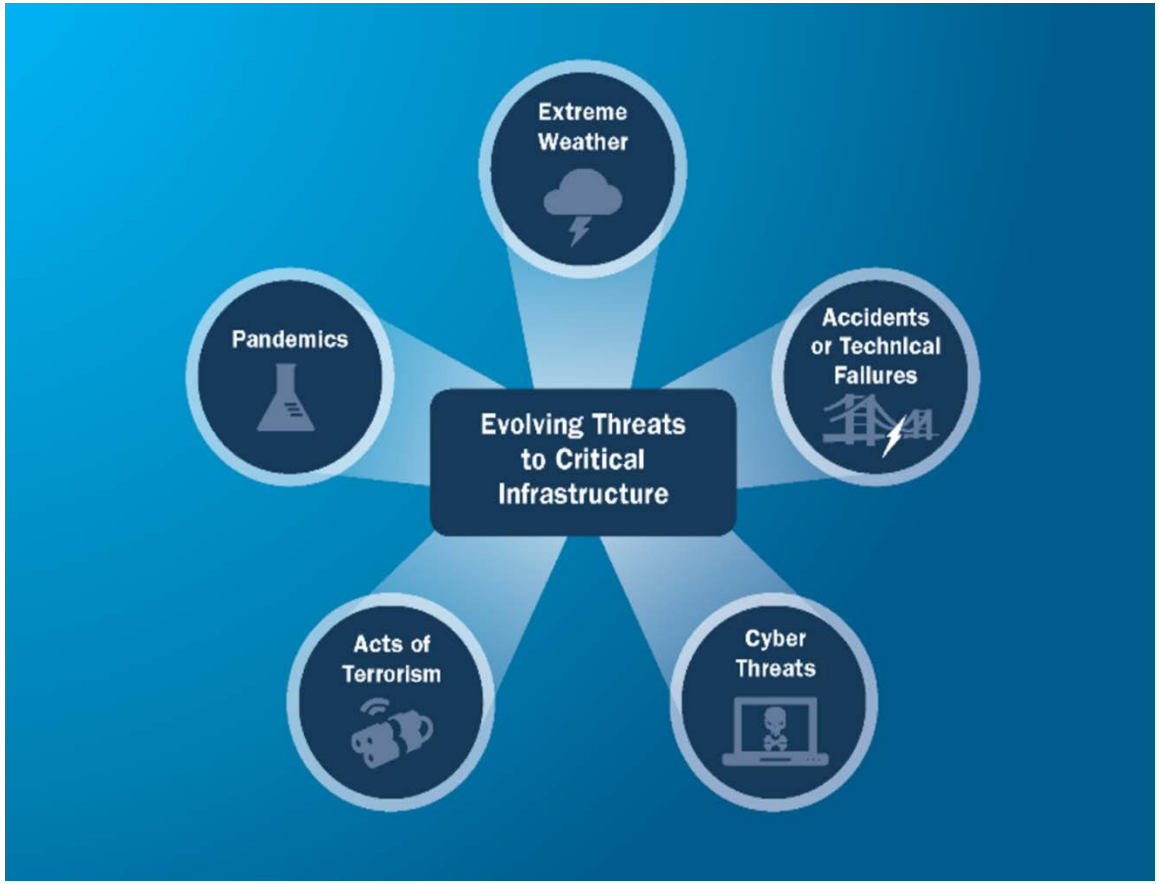
16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	DOT & DHS
WATER	EPA

Today's Risk Landscape

America remains at risk from a variety of threats including:

- Acts of Terrorism
- Cyber Attacks
- Extreme Weather
- Pandemics
- Accidents or Technical Failures
- International



Homeland Security Starts with Hometown Security

Security starts here.

connect plan train report

CISA
CYBER+INFRASTRUCTURE

For more information, visit
www.dhs.gov/hometown-security

if you SEE something | SAY something™

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

Homeland Security

What is Suspicious Activity?

Suspicious activity is only **behavior** that is reasonably indicative of criminal or terrorist-related activities.

Examples include someone:

- Leaving a backpack in an unattended place
- Trying to break into a restricted area

A person's race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity **must not** be considered as factors creating suspicion.

Reports based on appearance will only hinder law enforcement officers.

“If You See Something, Say Something”

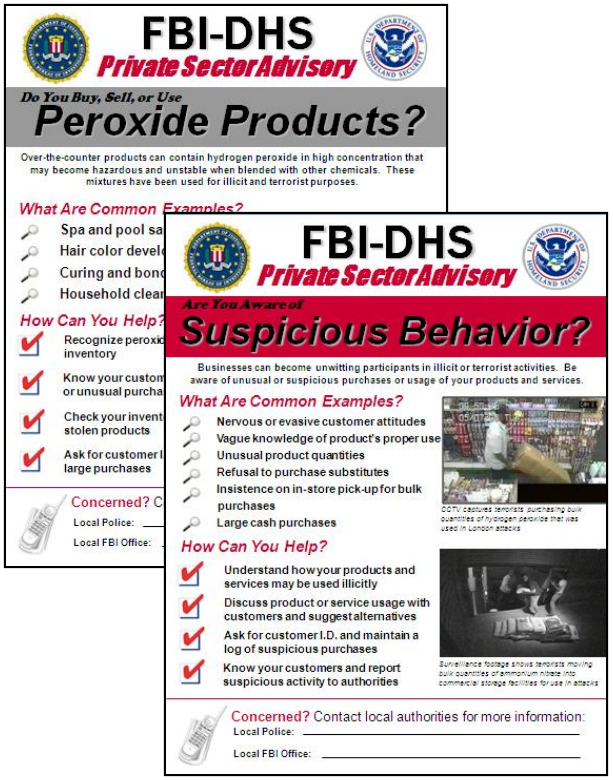
The following link takes you to the official webpage:

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

To become a partner, send an email to seesay@hq.dhs.gov and include:

- The entity you represent
- Your name and contact information (phone, email)
- The city and state in which your entity is located
- *Note: Locally customized posters and outreach materials are available to your organization*

Bomb-Making Materials Awareness Program

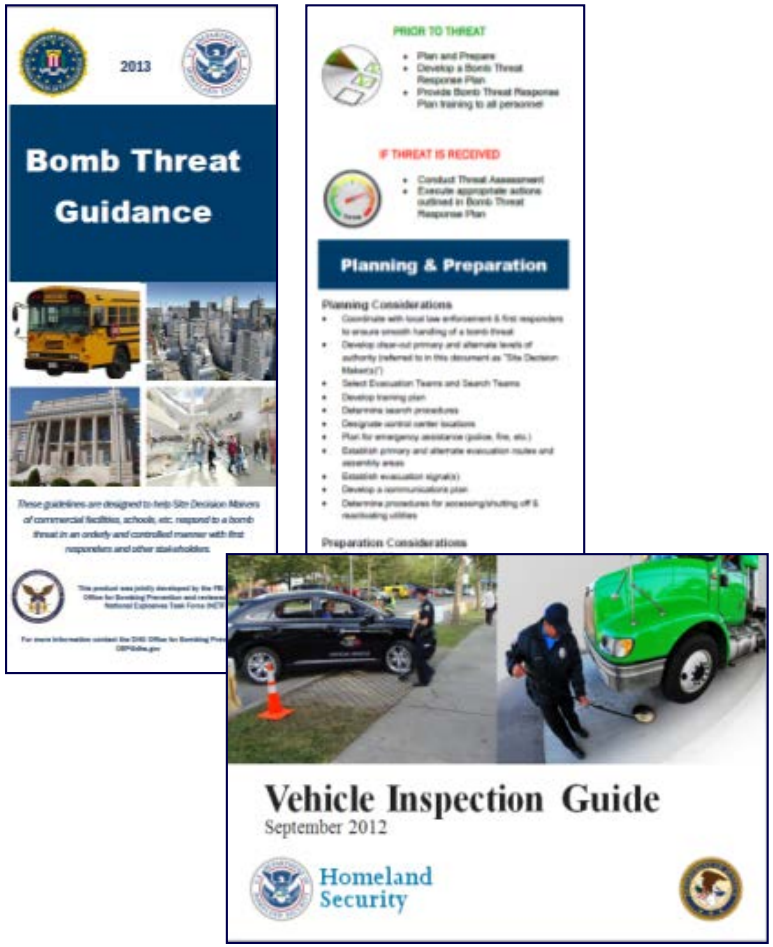


- **Overview:** Joint DHS-FBI program that promotes private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of dual-use explosive precursor chemicals and components commonly used in IEDs
- **Customers:** Private sector businesses and local law enforcement partners
- **Value:** Increases prevention opportunities by building a network of aware and vigilant private sector partners
- **Statistics:** 137 training events with 7,900+ State and local law enforcement and private sector partners since 2009

TSA: First Observer Plus™

- The First Observer Plus™ Program provides transportation professionals with the knowledge needed to recognize suspicious activity possibly related to terrorism, guidance in assessing what they see, and a method for reporting those observations.
- https://www.tsa.gov/for-industry/firstobserver

Transportation Security Administration



Courtesy of DHS OBP

- Bomb Threat Guidance provides a quick-reference for managing in-progress bomb threats for schools, businesses, and government facilities with information on police coordination, threat assessment, search, and evacuation versus shelter-in-place considerations
- Vehicle Inspection Guide assists Government and private sector security personnel in conducting vehicle inspection operations to prevent vehicle-borne IEDs

CISA
CYBER+INFRASTRUCTURE

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

HSIN

- https://hsin.dhs.gov/
- Homeland Security Information Network (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

Office of Bombing Prevention: Counter IED Training & Awareness

Courtesy of DHS OBP

- Diverse curriculum of training designed to build counter-IED core capabilities, such as:
  - *IED Countermeasures and Detection*
  - *Surveillance Detection Course*
  - *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 Virtual Instructor-Led Training (VILT) Awareness Courses available online

CISA
CYBER+INFRASTRUCTURE

CISA

CYBER+INFRASTRUCTURE