

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Title of session

Global Chemical Security Summit 2016

April 2016



Homeland
Security

Threats May Come from All Hazards



**Homeland
Security**

Department of Homeland Security

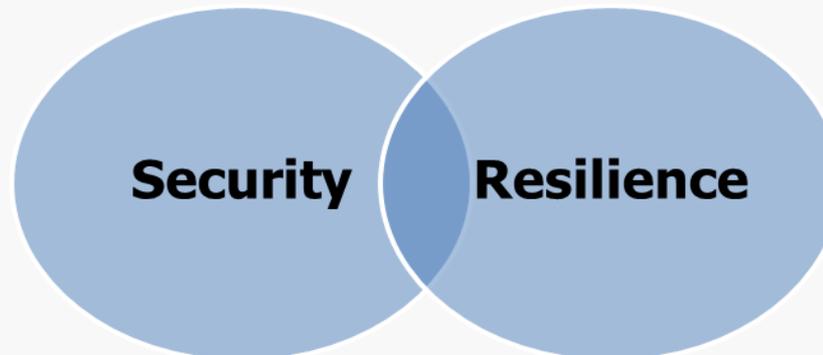


**Homeland
Security**

Infrastructure Protection (IP)

Overview

- Mission: To lead the national effort to mitigate risks to, strengthen the protection of, and enhance the all-hazard resilience of critical infrastructure
 - Resilience is the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies
- IP builds partnerships across the critical infrastructure domain, leads related preparedness activities, and serves as an information-sharing conduit between the private sector and public entities



**Homeland
Security**

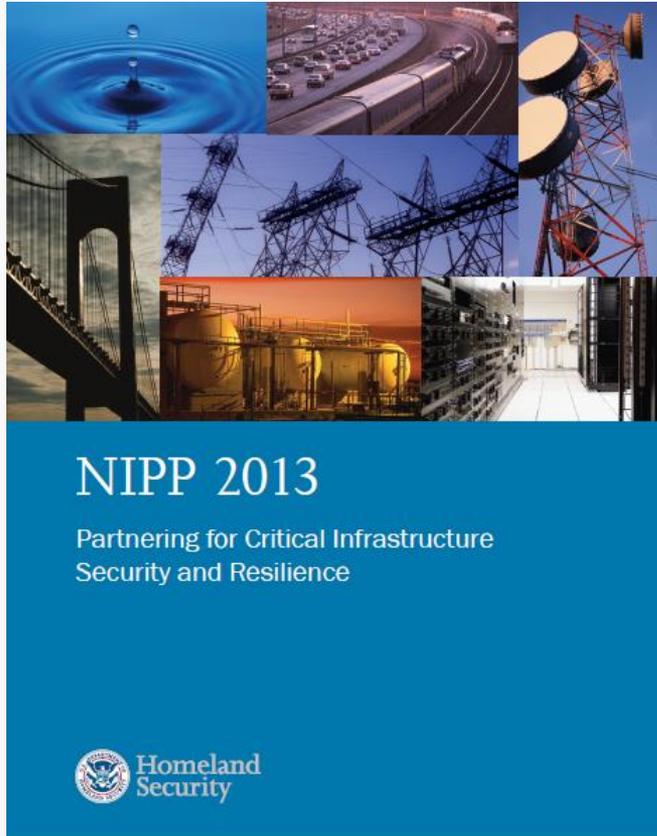
Office of Infrastructure Protection Services

- Partnerships and Information Sharing
- Voluntary Programs



**Homeland
Security**

National Infrastructure Protection Plan



Courtesy of DHS

- Comprehensive plan for the public and private sector to enhance critical infrastructure protection and resilience:
 - Partnership model
 - Risk management framework
 - Roles, responsibilities, and authorities
- Guides internal DHS programs and activities and those of:
 - Other Federal agencies and departments
 - State, local, tribal, and territorial governments
 - Critical infrastructure owner and operators
- NIPP 2013 vision:
 - “A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.”



**Homeland
Security**

Many Stakeholders, Many Strengths

Comparative Advantage

- Engaging in collaborative process
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness

Owner-Operators

Customer Relations
Operations
Investment

State, Local, Regional

Emergency Management
Utility Regulation
Public Safety
Law Enforcement



Federal Government

National Policy
Information Sharing
Coordination

NGOs

Trusted Relationships
Community Building
Resilience



**Homeland
Security**

Partnerships and Key Stakeholders

- Owners and operators of critical infrastructure assets and systems
- State, local, territorial and tribal governments
 - State Environmental Agencies, Homeland Security Advisors
 - Local Emergency Managers, Law Enforcement
- Other Federal partners
 - Intelligence Community
 - Federal Law Enforcement
 - Emergency Management
 - Regulatory Agencies



**Homeland
Security**

Information Sharing

- National Infrastructure Coordinating Center (NICC):
 - Maintains operational and situational awareness of the Nation's critical infrastructure resources through the 24/7 watch and operations center and Critical Infrastructure Crisis Action Team



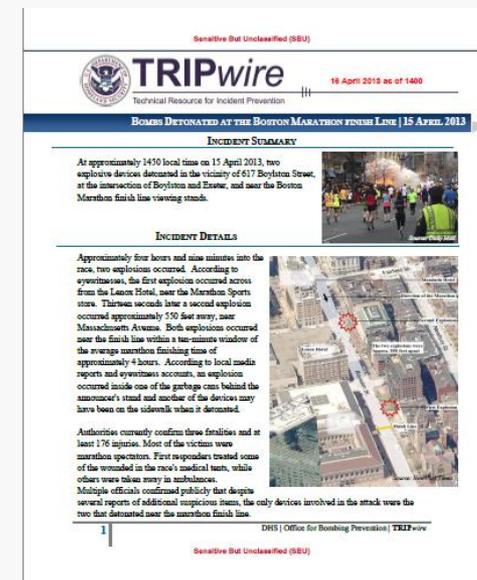
- Homeland Security Information Network – Critical Sectors:
 - Information sharing collaboration platform that provides tactical and planning information for owners and operators and government partners of critical infrastructure



Homeland
Security

Technical Resource for Incident Prevention (TRIPwire)

- **Overview:** Secure information sharing platform for IED incident information, evolving IED tactics, incident lessons learned, and counter-IED preparedness information
- **Customers:** State and local law enforcement and emergency services; Federal agencies; and private sector
- **Value:** Provides access to counter-IED information and resources to build knowledge and preparedness capabilities, filling vital gaps in information sharing

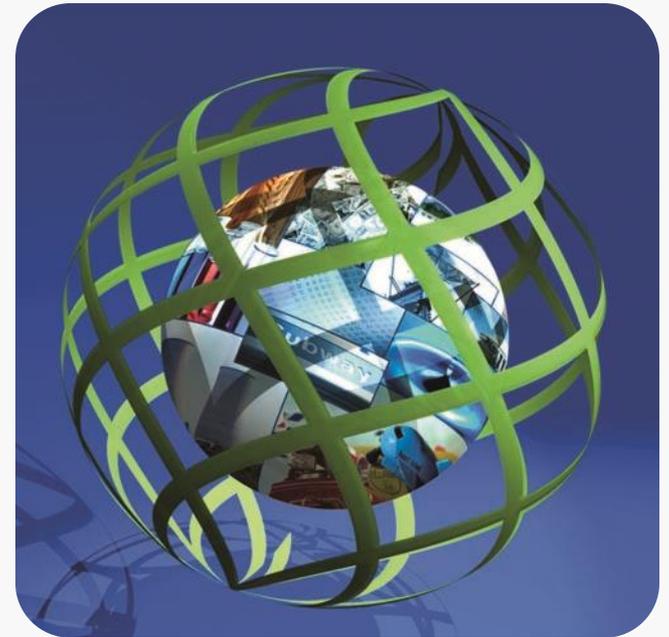


Homeland
Security

FOR OFFICIAL USE ONLY

Protected Critical Infrastructure Information

- The Protected Critical Infrastructure Information (PCII) Program protects voluntarily submitted critical infrastructure information through exemption from:
 - State and local disclosure laws
 - Use in civil litigation
 - Regulatory use



Enhanced Critical Infrastructure Protection (ECIP) Initiative

- Voluntary program to educate critical infrastructure owner/operators on the importance of their facilities and available DHS resources
- ECIP briefing
 - Inform and educate facility owners
 - Discuss critical dependencies/interdependencies
 - Provide access to DHS training and resources
 - Strengthen cooperation and stakeholder awareness
- ECIP security survey
 - Infrastructure Survey Tool (IST)
 - In-depth knowledge of the current facility security and resilience posture
 - Document facility capabilities and dependencies for incident response
 - Interactive dashboard



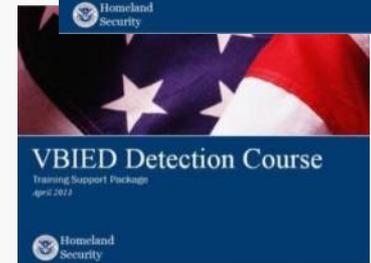
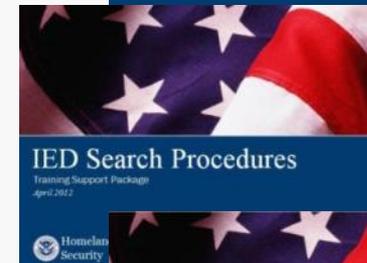
Regional Resiliency Assessment Program (RRAP)

- The goal of the RRAP is to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen resilience to all hazards
 - Achieved through a combination of vulnerability assessments, regional analysis, and research related to the RRAP focus area
- The RRAP process identifies critical infrastructure security, resilience, dependencies, interdependencies, cascading effects, and State, local, tribal, and territorial agency capability gaps
- Resiliency Assessment Report
 - RRAP key findings; Follow-up activities; Engagement with States and key stakeholders



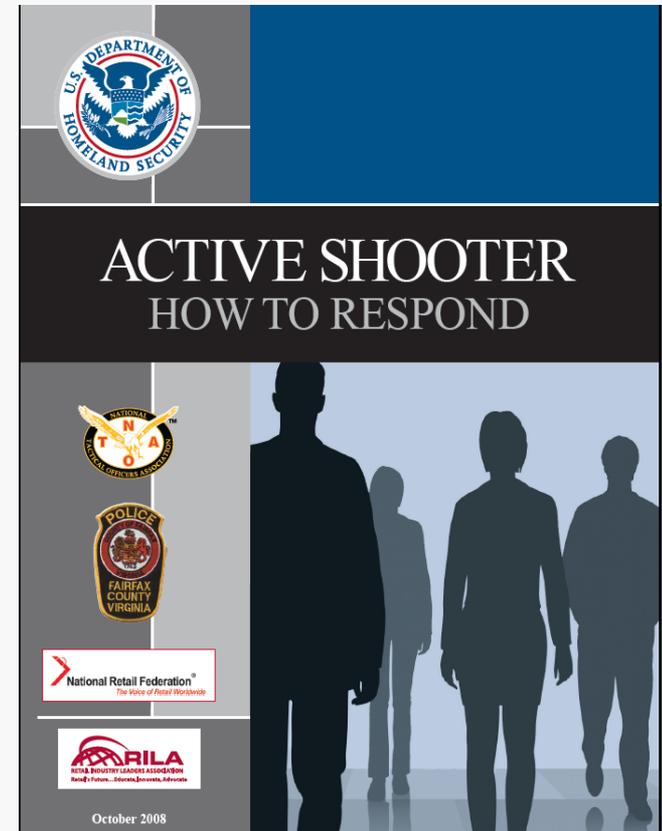
Counter-Improvised Explosive Device Training and Awareness

- Overview: Diverse curriculum of training designed to build counter-IED core capabilities, such as:
 - Surveillance Detection
 - Protective Measures
 - IED Awareness
 - Bomb Threat Management
 - Vehicle-Borne IED (VBIED) Detection
 - IED Search Procedures
 - IED Counterterrorism
- Customers: State and local law enforcement and first responders; Federal agencies; and private sector partners
- Value: Increases knowledge and ability to detect, prevent, protect against, and respond to bombing threats



Active Shooter Outreach

- IP has developed a multimedia package and training to assist critical infrastructure owners and operators in preparing for and responding to an active shooter in their facility
 - Desk reference guide, a reference poster, and a pocket-size reference card.
 - Independent Study Course
 - Active Shooter Webinar
 - Active Shooter Workshop Series
- Partnered with FEMA's Emergency Management Institute to produce the free, online independent study course:
- All Active Shooter resources can be found at:
www.dhs.gov/active-shooter-preparedness



**Homeland
Security**

See Something Say Something



“If You See Something, Say Something” is a national 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.

- Launched in July of 2010 by DHS, in conjunction with the U.S. Department of Justice’s Nationwide Suspicious Activity Reporting Initiative (NSI), with the goal of training state and local law enforcement to recognize behaviors and indicators of terrorism and terrorism-related crime.
- The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners.
 - Provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.



**Homeland
Security**

www.dhs.gov/See-Something-Say-Something

Protective Security Advisors

- 96 Protective Security Advisors (PSAs) and Regional Directors (RDs), including 89 field deployed personnel, serve as critical infrastructure security specialists
- State, local, tribal, territorial, 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 and the Federal Emergency Management Agency



Chemical Sector Voluntary Security Programs

- Security Seminar and Workshop Series:
 - Encourages facility owner and operators and their security partners to collaborate
- Tabletop Exercise Program
 - Unclassified, adaptable exercises that provide an opportunity for partners to address gaps, threats, issues, and concerns
- Chemical Security Awareness Training
 - Helps to increase security awareness at chemical facilities
- Annual Chemical Sector Security Summit



**Homeland
Security**



Chemical Sector Voluntary Security Programs cont.

- Chemical Sector Industrial Control Systems Security Resource
 - Collection of training and reference information designed to assist owners and operators in addressing Industrial Control Systems (ICS) security
- Suspicious Activity Reporting Teleconference
 - Monthly, unclassified threat briefing and suspicious activity reporting teleconference for chemical and oil and national gas facility owners and operators as well as supply-chain manufacturers
- Chemical Sector-Specific Plan
 - Completed through a coordinated effort involving public and private sector partners and details how the risk management framework is implemented



Chemical Sector-Specific Plan

An Annex to the NIPP 2013

2015



Homeland
Security



Homeland
Security



Homeland Security

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

Sarah Gambill

Infrastructure Development and
Recovery Chief

Sarah.Gambill@hq.dhs.gov



Homeland
Security

Regulatory
Programs

Federal Voluntary
Programs

Industry Programs



**Homeland
Security**