The Office of Infrastructure Protection

National Protection and Programs Directorate (NPPD)
Department of Homeland Security (DHS)

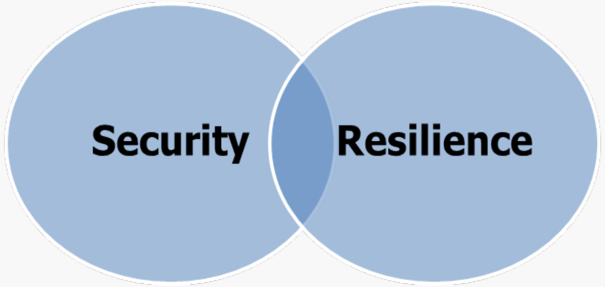
Voluntary Programs

June 2018

Homeland Security

Office of Infrastructure Protection (IP)

- Mission: To lead the national effort to secure critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community

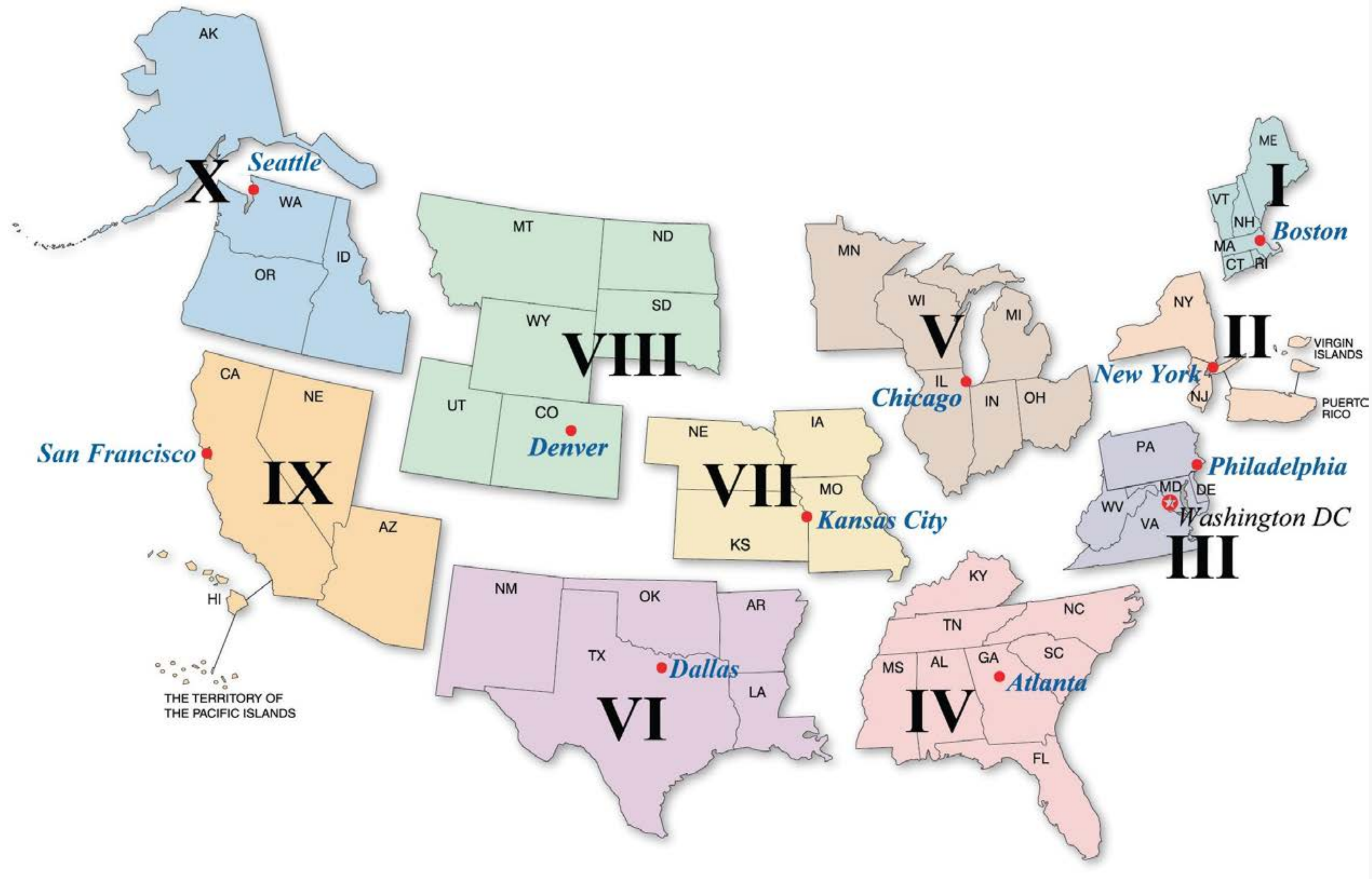


- IP builds partnerships across the critical infrastructure domain, leads related preparedness activities, and serves as an information sharing conduit between the private sector and public entities

Regionalizing the Infrastructure Protection Mission

- The Office of Infrastructure Protection (IP) has established regional offices to improve the delivery of services to stakeholders and existing field forces.
- Key attributes and enhanced operations include:
  - Co-location of mission support staff
  - Decentralization of outreach, exercises, analysis, and training currently performed at headquarters
  - Enhanced coordination during steady state, special events, and incident response
  - Better customer service to public and private stakeholders

IP Regions



Courtesy of DHS

Protective Security Advisors (PSAs)

- Field-deployed personnel who serve as critical infrastructure security specialists
- Serve as State, local, tribal, and territorial government and private sector link to DHS infrastructure protection resources:
    - Coordinate voluntary assessments, training, and other DHS products and services
    - Provide a vital link for information sharing in steady state and incident response
    - Assist facility owners/operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts of the States

Cyber Security Advisors (CSAs)

- Regionally located DHS personnel assigned to districts throughout the Nation
- 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 State, local, territorial, and tribal governments
- Offer immediate and sustained assistance to prepare/protect State, local, territorial, and tribal governments and private sector entities
- Bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer alignment with the Federal government

For more information about the CSA Program, email cyberadvisor@hq.dhs.gov

For more information on DHS cyber programs, visit www.dhs.gov/cyber

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

Courtesy of DHS

Homeland Security

Security and Resilience Challenges

- A majority of critical infrastructure is privately owned
- DHS has limited legal authority to regulate security practices of private industry
- DHS, Sector-Specific Agencies (SSAs), other Federal entities, the private sector, and State, local, tribal, and territorial governments all have roles and responsibilities in critical infrastructure protection

Sector-Specific Agencies (SSAs)

- SSAs are the primary Federal entities responsible for coordinating critical infrastructure security and resilience efforts within individual sectors
- DHS is the SSA for 10 of the 16 sectors
- Facilitate the public-private partnership across critical infrastructure sectors
- Develop strategic goals to mitigate risk and improve resilience

Homeland Security

Sector-Specific Agencies (cont.)

- Provide and promote education, training, information sharing, and outreach support
- Shape sector-specific goals that address physical, human, and cybersecurity risks and drive security and resilience activities and programs
- Provide, support, and facilitate technical assistance and consultations to identify vulnerabilities and help mitigate incidents

Chemical Sector-Specific Agency Voluntary Programs *

Courtesy of DHS

- The Chemical SSA supports requests from chemical industry councils, associations, and emergency management agencies for presentations, training, exhibits, and exercises to improve the security and resilience of the chemical industry

Chemical Sector Information-Sharing Avenues

- Biennial Chemical Sector Security Summit – IP and Chemical Sector Coordinating Council (SCC) co-host the annual Summit, which consists of workshops, presentations, and discussions
  - Topics include Chemical Facilities Anti-Terrorism Standards (CFATS) overview, cybersecurity, theft and diversion, local resources, and several workshops
- Threat and Suspicious Activity Reporting Teleconference – DHS hosts a monthly unclassified threat briefing and suspicious activity reporting teleconference for chemical facility owners and operators
  - To participate, apply for access to the Homeland Security Information Network (HSIN). Visit www.dhs.gov/hsin-critical-infrastructure for more information.

Chemical Sector Information-Sharing Avenues (cont.)

- Classified Briefings – As needed, the Chemical SSA sponsors classified briefings where the intelligence community provides information on both physical and cyber threats for cleared industry representatives

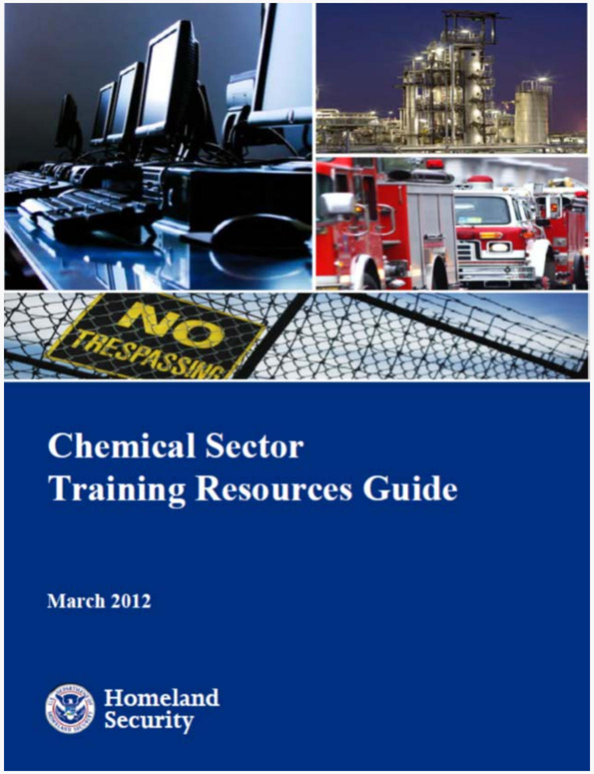
- Homeland Security Information Network – Critical Infrastructure (HSIN-CI) – The primary information-sharing platform for the Chemical Sector
  - The sector uses HSIN during incidents

- Government Coordinating Council (GCC)/SCC Meetings – The Chemical GCC and SCC meet to discuss current security issues that impact the sector

Chemical Sector Training Resource Guide

- The guide contains a list of free or low-cost voluntary training, web-based classes, seminars, and documents routinely available through several component agencies within DHS

- The guide was compiled to assist facility security officers train their employees on industry best practices, physical and cybersecurity awareness, and emergency management and response



Chemical Sector
Training Resources Guide

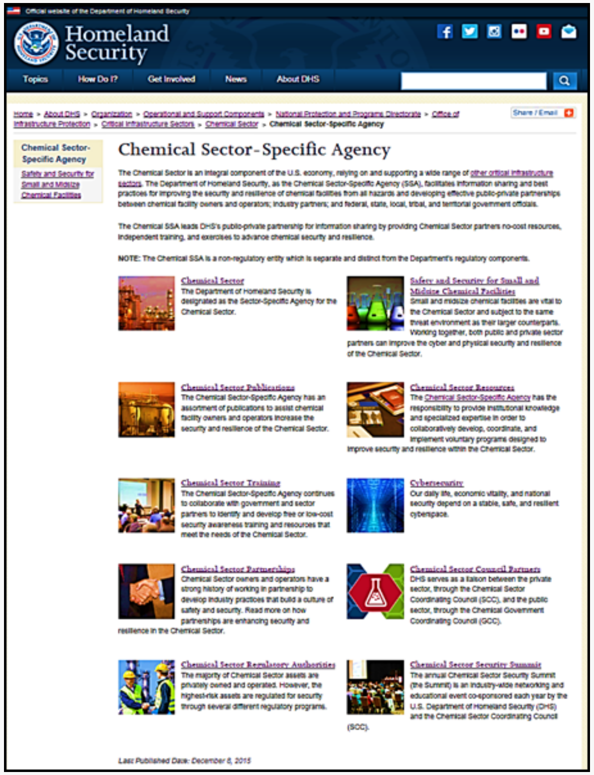
March 2012

Homeland
Security

Courtesy of DHS

Chemical Sector-Specific Agency Landing Page

- DHS Office of Infrastructure Protection, Chemical SSA has a newly developed landing page which consists of thumbnails and brief descriptions of an entire suite of new and updated information-sharing resources
- www.dhs.gov/chemical-sector



Home > About DHS > Organization > Operational and Support Components > National Protection and Programs Directorate > Office of Infrastructure Protection > Critical Infrastructure Sectors > Chemical Sector > Chemical Sector-Specific Agency

Chemical Sector-Specific Agency
Safety and Security for Small and Midsize Chemical Facilities

Chemical Sector-Specific Agency

The Chemical Sector is an integral component of the U.S. economy, relying on and supporting a wide range of other critical infrastructure sectors. The Department of Homeland Security, as the Chemical Sector-Specific Agency (SSA), facilitates information sharing and best practices for improving the security and resilience of chemical facilities from all hazards and developing effective public-private partnerships between chemical facility owners and operators; industry partners; and federal, state, local, tribal, and territorial government officials.

The Chemical SSA leads DHS's public-private partnership for information sharing by providing Chemical Sector partners no-cost resources, independent training, and exercises to advance chemical security and resilience.

NOTE: The Chemical SSA is a non-regulatory entity which is separate and distinct from the Department's regulatory components.

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Safety and Security for Small and Midsize Chemical Facilities
Small and midsize chemical facilities are vital to the Chemical Sector and subject to the same threat environment as their larger counterparts. Working together, both public and private sector partners can improve the cyber and physical security and resilience of the Chemical Sector.

Chemical Sector Publications
The Chemical Sector-Specific Agency has an assortment of publications to assist chemical facility owners and operators increase the security and resilience of the Chemical Sector.

Chemical Sector Resources
The Chemical Sector-Specific Agency has the responsibility to provide institutional knowledge and specialized expertise in order to collaboratively develop, coordinate, and implement voluntary programs designed to improve security and resilience within the Chemical Sector.

Chemical Sector Training
The Chemical Sector-Specific Agency continues to collaborate with government and sector partners to identify and develop free or low-cost security awareness training and resources that meet the needs of the Chemical Sector.

Cybersecurity
Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

Chemical Sector Partnerships
Chemical Sector owners and operators have a strong history of working in partnership to develop industry practices that build a culture of safety and security. Read more on how partnerships are enhancing security and resilience in the Chemical Sector.

Chemical Sector Council Partners
DHS serves as a liaison between the private sector, through the Chemical Sector Coordinating Council (SCC), and the public sector, through the Chemical Government Coordinating Council (GCC).

Chemical Sector Regulatory Authorities
The majority of Chemical Sector assets are privately owned and operated. However, the highest-risk assets are regulated for security through several different regulatory programs.

Chemical Sector Security Summit
The annual Chemical Sector Security Summit (the Summit) is an industry-wide networking and educational event co-sponsored each year by the U.S. Department of Homeland Security (DHS) and the Chemical Sector Coordinating Council (SCC).

Last Published Date: December 8, 2015

Courtesy of DHS

Online Voluntary Security Awareness Training

- IS-916: Theft and Diversion – What You Can Do

  Identifies threats and vulnerabilities to critical infrastructure from the theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. Identifies actions that participants can take to reduce or prevent theft and diversion.

- IS-914: Surveillance Awareness: What You Can Do

  Makes critical infrastructure employees and service providers aware ways to detect and report suspicious activities associated with adversarial surveillance.

- IS-906: Workplace Security Awareness

  Security threats endanger the confidentiality, integrity, and security of your workplace, as well as your virtual workplace and computer systems. Presents information on how employees can contribute to your organization's security.

Online Voluntary Security Awareness Training

- IS-915: Protecting Critical Infrastructure Against Insider Threats

  Provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure.

- Critical Infrastructure Foundational Courses
- Security Awareness Courses
- Training available at http://training.fema.gov/IS/CISR.aspx

Cybersecurity Voluntary Resources

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-Computer Emergency Readiness Team (CERT) Operations Center
    - Remote and Onsite Assistance
    - Malware Analysis
    - Incident Response Teams
  - Industrial Control Systems (ICS)-CERT Operations Center
    - ICS-CERT Malware Lab
    - Cyber Security Evaluation Tool
    - Incident Response Teams

Homeland Security

Cyber Incident Reporting

- NCCIC provides real-time threat analysis and incident reporting capabilities
  - 24x7 contact number: 1-888-282-0870
  - forms.us-cert.gov/report/

- When to report:
  - If there is a suspected or confirmed cyberattack 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

Chemical Sector Industrial Control Systems Security Resource

Chemical Sector Industrial Control Systems Security Resource
October 2011
Chemical Sector
U.S. Department of Homeland Security
Office of Infrastructure Protection
DVD
Homeland Security

- Case for Action
- Roadmap to Secure Control Systems in the Chemical Sector
- Cyber Assessments
- Cybersecurity Tabletop Exercise
- ISC – Cyber Emergency Team
- Procurement Language
- ICS Security Training
- Intrusion Detection
- Standards and Guidelines

Homeland Security

Most of these resources can be found at:
http://www.chemicalcybersecurity.org/RESOURCES-And-TOOLS

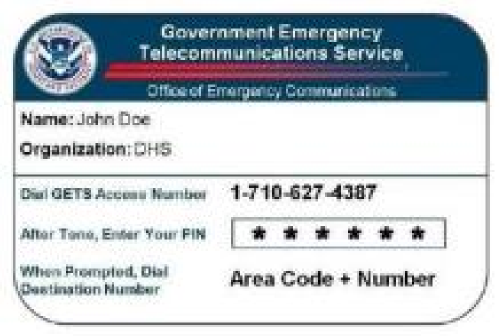
InfraGard

- InfraGard is an information-sharing and analysis effort serving the interests of and combining the knowledge base of a wide range of members
- InfraGard is a partnership between the Federal Bureau of Investigation 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
- For more information, visit www.infragard.org

DHS Office of Emergency Communications (EOC) Priority Telecommunications Services

Priority Telecommunications Services provide public safety and National Security/Emergency Preparedness users the ability to communicate on telecommunications networks during times of congestion

- GETS: Government Emergency Telecommunications Service
- WPS: Wireless Priority Service
- TSP: Telecommunications Service Priority



Government Emergency Telecommunications Service

Office of Emergency Communications

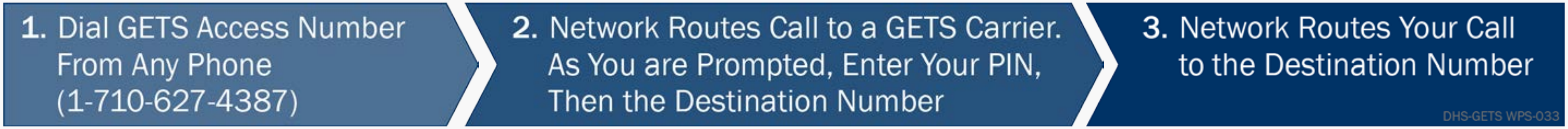
Name: John Doe

Organization: DHS

Dial GETS Access Number	1-710-627-4387
After Tone, Enter Your PIN	* * * * * *
When Prompted, Dial Destination Number	Area Code + Number

GETS: Solution for Wireline Congestion

- GETS provides priority access to the landline networks when abnormal call volumes exist, providing enhanced call completion for critical personnel.
- Provides priority treatment of calls over the commercial telephone network - not a separate system
- Priority through the public switched telephone network and priority to called WPS enabled carriers
- Designed to provide over 90% call completion rates: 95% of GETS calls were completed during Hurricanes Isaac, Irene, and Sandy



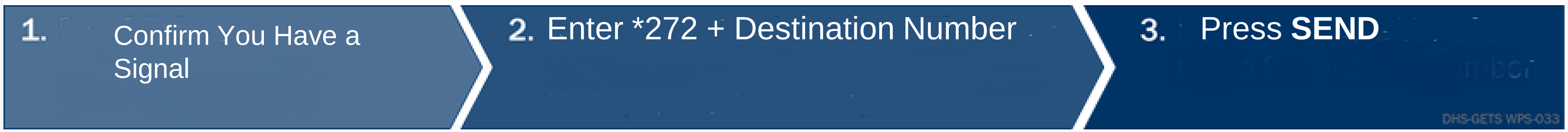
1. Dial GETS Access Number From Any Phone (1-710-627-4387)
2. Network Routes Call to a GETS Carrier. As You are Prompted, Enter Your PIN, Then the Destination Number
3. Network Routes Your Call to the Destination Number

www.dhs.gov/gets

WPS: Solution for Wireless Congestion

- WPS provides priority voice access to the cellular networks when abnormal call volumes exist, providing enhanced call completion for critical public safety personnel.

- Available on all the major cellular carriers and some regional cellular carriers
- WPS is an add-on feature to an approved phone and must be added to each applicable cell phone subscription
- Designed to provide 80% call completion rates: during Hurricane Sandy, over 98% of WPS calls were completed



1. Confirm You Have a Signal
2. Enter *272 + Destination Number
3. Press **SEND**

www.dhs.gov/wps

Homeland Security

TSP: Provisioning and Restoration

- Provisioning
  - TSP authorizes priority installation of new voice and data circuits
  - Cannot be used to compensate for inadequate planning
- Restoration
  - Organizations designate critical circuits to have priority repair and restoration if damaged
  - Circuits must be registered with TSP prior to requesting priority restoration

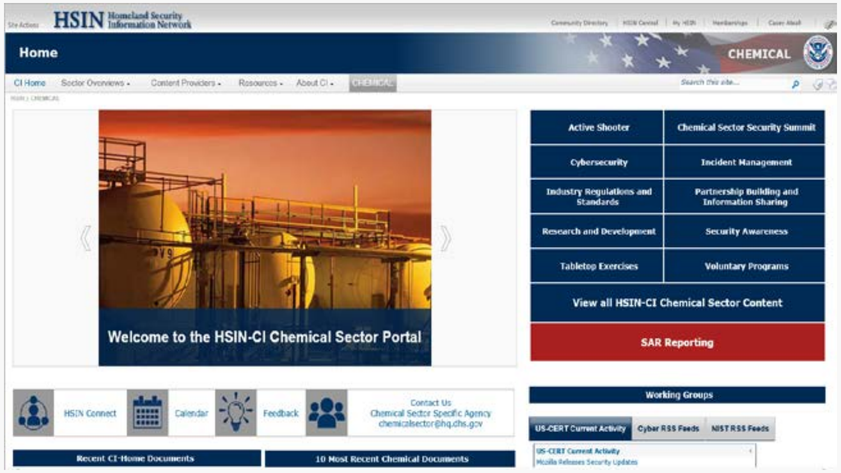
www.dhs.gov/tsp

Homeland Security

HSIN-CI Chemical Sector

The Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Chemical Sector is a secure portal that provides a “peer-to-peer” collaboration space for members to engage in real-time

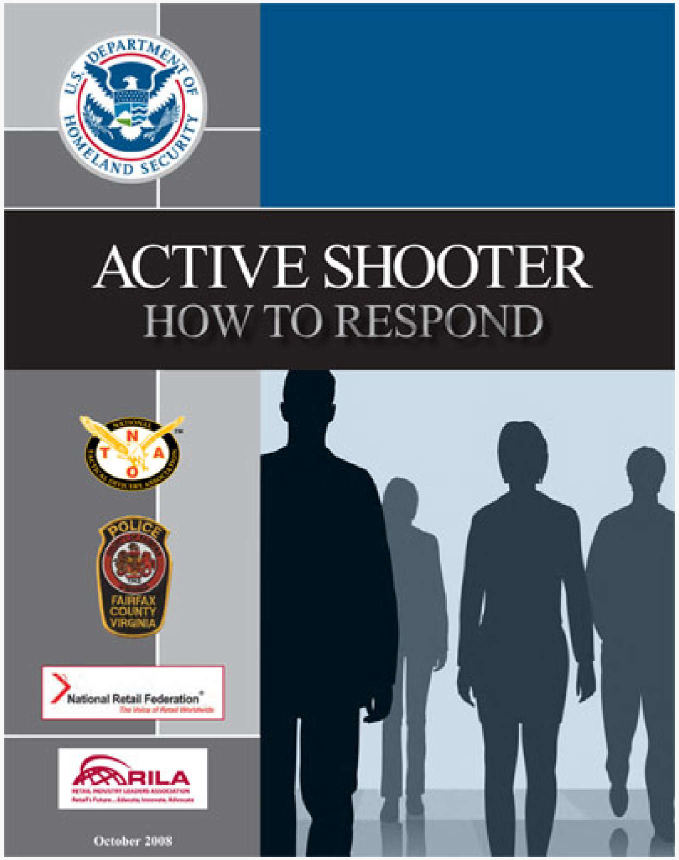
- Resources available on the HSIN-CI include analysis, alerts, bulletins, training, exercise materials and Suspicious Activity Reporting.
- **For Access** to HSIN-CI please email the below information to HSINCI@hq.dhs.gov:
    - Your full name, employer, work email address, sector


HSIN Homeland Security Information Network
Site Actions
Community Directory | HSIN Central | My HSIN | Memberships | Cases Alert
Home
CHEMICAL
CI Home
Sector Overviews
Content Providers
Resources
About CI
CHEMICAL
Search this site...
Welcome to the HSIN-CI Chemical Sector Portal
Active Shooter
Chemical Sector Security Summit
Cybersecurity
Incident Management
Industry Regulations and Standards
Partnership Building and Information Sharing
Research and Development
Security Awareness
Tabletop Exercises
Voluntary Programs
View all HSIN-CI Chemical Sector Content
SAR Reporting
HSIN Connect
Calendar
Feedback
Contact Us
Chemical Sector Specific Agency
chemicalsector@hq.dhs.gov
Working Groups
US-CERT Current Activity
Cyber RSS Feeds
NIST RSS Feeds
US-CERT Current Activity
Mozilla Releases Security Updates
Recent CI-Home Documents
10 Most Recent Chemical Documents

Courtesy of DHS

Homeland Security

Active Shooter Preparedness – Resources and Materials



ACTIVE SHOOTER
HOW TO RESPOND

October 2008

U.S. DEPARTMENT OF HOMELAND SECURITY
N T A O
POLICE
FAIRFAX COUNTY VIRGINIA
National Retail Federation
RILA

- Provide private sector partners with the tools needed to prepare and train for an active shooter incident
- Materials consists of three products:
  - Basic Guide Book
  - Break Room poster
  - Pocket Emergency Measures Guide
- www.dhs.gov/activeshooter

Active Shooter Preparedness – Online Training

- **Active Shooter, What You Can Do (IS-907)**
- Provides the public with guidance on how to prepare for and respond to active shooter crisis situation https://training.fema.gov/is/courseoverview.aspx?code=IS-907.
- Upon completion employees and managers will be able to:
  - Describe the actions to take when confronted with an active shooter and to assist responding law enforcement officials;
  - Recognize potential workplace violence indicators;
  - Describe actions to take to prevent and prepare for potential active shooter incidents; and
  - Describe how to manage the consequences of an active shooter incident.

Active Shooter Emergency Action Plan Video

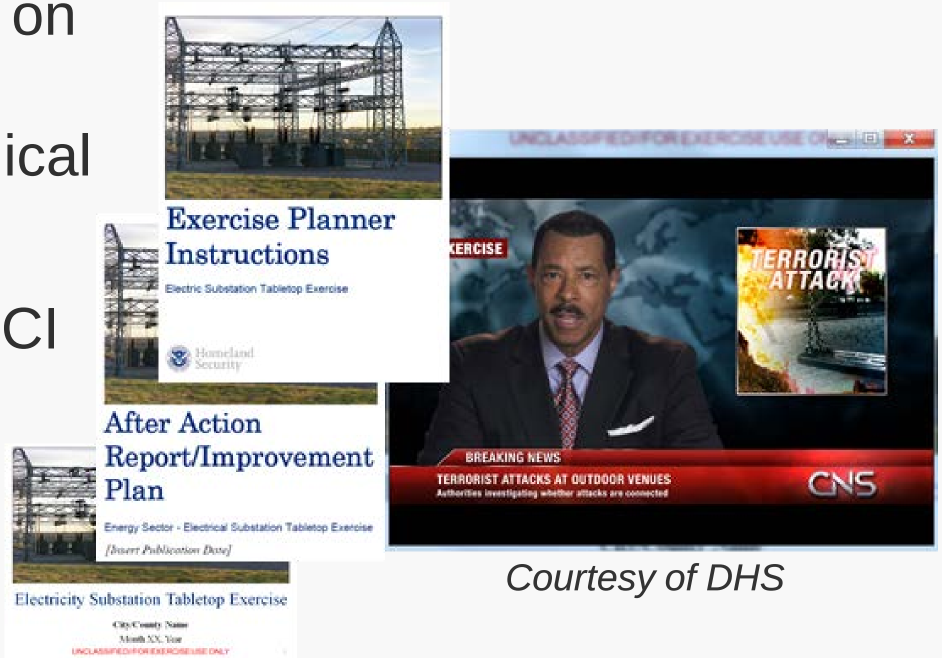
- The Active Shooter Emergency Action Plan Video describes the fundamental concepts of developing an Emergency Action Plan (EAP) for an active shooter scenario.
- The instructive video guides viewers through important considerations of EAP development utilizing the first-hand perspectives of active shooter survivors, first responder personnel, and other subject matter experts who share their unique insight.
- Available on https://www.dhs.gov/active-shooter-workshop-participant

Active Shooter Preparedness – Workshops

- DHS conducts one-day Active Shooter Preparedness Workshops across the country to enhance awareness of, and response to, an active shooter event
- Upon completion of the workshop corporate and facility security professionals from the private and public sector will be able to develop an Active Shooter Preparedness plan that addresses:
  - Incident Pre-Planning
  - Incident Response Considerations
  - Incident Recovery Considerations
  - Business Continuity
  - Employee training
  - Training and Exercise Plan
  - Incorporating lessons learned into current plans
- Workshop curriculum is available on www.dhs.gov/activeshooter.

Sector-Specific Tabletop Exercise Program (SSTEP)

- Provides easily modified “prepackaged” tabletop exercises (TTX) for Chemical sector to utilize “off-the-shelf”
- Opportunity for stakeholders and their public partners to focus on gaps, threats, issues, and concerns affecting the Chemical Sector
- Materials available on HSIN-CI



Exercise Planner Instructions

Electric Substation Tabletop Exercise

Homeland Security

After Action Report/Improvement Plan

Energy Sector - Electrical Substation Tabletop Exercise

[Insert Publication Date]

Electricity Substation Tabletop Exercise

City/County Name

Month XX, Year

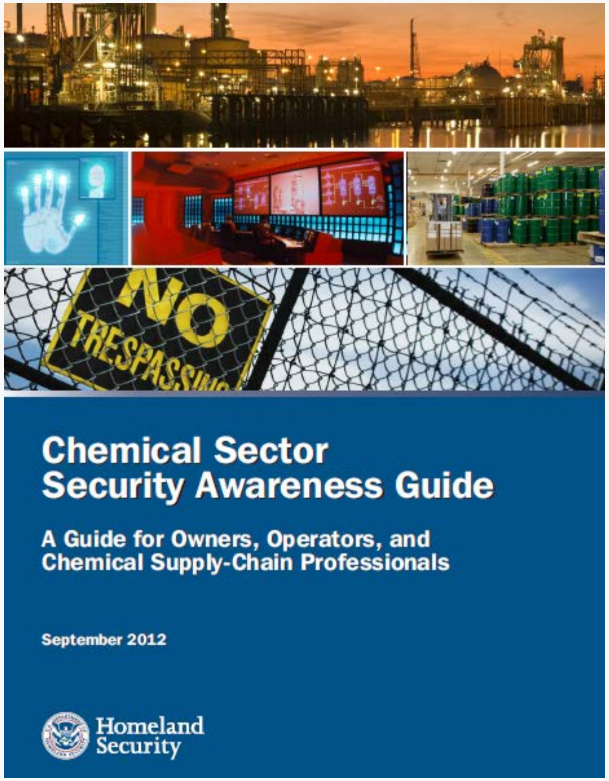
UNCLASSIFIED//FOR EXERCISE USE ONLY

UNCLASSIFIED//FOR EXERCISE USE ONLY
XERCISE
TERRORIST ATTACK
BREAKING NEWS
TERRORIST ATTACKS AT OUTDOOR VENUES
Authorities investigating whether attacks are connected
CNS

Courtesy of DHS

Chemical Sector Security Awareness Guide

A compiled list of free or low-cost training, Web-based classes, and seminars that are routinely available through one of several component agencies within DHS.



Chemical Sector Security Awareness Guide

A Guide for Owners, Operators, and Chemical Supply-Chain Professionals

September 2012

Homeland Security

Courtesy of DHS

Homeland Security

Counter-Improvised Explosive Device (IED) Training and Awareness

Protective Measures Course
Training Support Package
September 2012
Homeland

IED Search Procedures
Training Support Package
April 2012
Homeland Security

Bomb Threat Management
Training Support Package
January 2013
Homeland Security

VBIED Detection Course
Training Support Package
April 2013
Homeland Security

Courtesy of DHS

- Diverse training curriculum 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
- Courses are taught around the United States in a traditional classroom setting by a mobile training team, through online computer-based training, through a virtual instructor-led training (VILT) platform, and in-resident training courses at FEMA's Center for Domestic Preparedness

Homeland Security

Online Counter-IED Virtual Instructor-Led Training (VILT)

- **AWR-338 Homemade Explosives (HME) and Precursor Awareness**

  Provides foundational knowledge on HME and common chemical precursors and other materials used to construct IEDs.

- **AWR-334 Introduction to the Terrorist Attack Cycle Course**

  Introduces a conceptual model of common steps in planning and executing terrorist attacks. Describes the nature of terrorist surveillance, target selection, planning, and other activities that occur before and immediately after an attack.

- **AWR-333 Improvised Explosive Device (IED) Construction and Classification Course**

  Provides participants with foundational knowledge on the construction and classification of IEDs, including their function, components, classifications, and how they are constructed.

Homeland Security

To view the VILT training schedule and register for a course, go to https://cdp.dhs.gov/obp

Online Counter-IED Virtual Instructor Led Training (VILT) (cont.)

- **AWR-337 Improvised Explosive Device (IED) Explosive Effects Mitigation Course**

  Introduces participants to the effects of an explosive blast; details the difference between blast, thermal/incendiary, and fragmentation effects; and describes the destructive consequences of each type of effect on the target.

- **AWR-340 Protective Measures Awareness Course**

  Provides participants foundational knowledge on terrorist planning cycle, risk management, surveillance detection, and various protective measures.

- **AWR-335 Response to Suspicious Behaviors and Items Course**

  Provides an overview of suspicious behavior indicators and appropriate responses to suspicious behaviors and items.

To view the VILT training schedule and register for a course, go to https://cdp.dhs.gov/obp

Homeland Security

Online Counter-IED Awareness Training

- **AWR-341 IED Awareness and Safety Procedures**

  The purpose of this course is to provide the foundational knowledge about improvised explosive devices (IEDs) and proper safety precautions and procedures for reacting and responding to unattended and suspicious items.

- **AWR-349 Homemade Explosives and Precursor Chemicals Awareness for Public Safety**

  The purpose of this course is to educate law enforcement, firefighters, emergency medical technicians, and other public safety personnel about homemade explosives – commonly referred to as HME – and the precursor chemicals that are used to manufacture HME. The CBT includes information about HME dangers, who manufacturers them, what to look for on a call, and actions to take if HME precursor chemicals or equipment are thought to be present during a routine service call.

OBP computer based training courses are available on tripwire.dhs.gov/

Homeland Security

Infrastructure Protection Report Series (IPRS)

Characteristics and Common Vulnerabilities

Protective Measures

Potential Indicators of Terrorist Activity

Courtesy of DHS

- 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
- Please email PSCDOperations@hq.dhs.gov for information on how to access the IPRS

National Infrastructure Coordinating Center (NICC)

- The NICC is the information and coordination hub of a national network dedicated to protecting critical infrastructure
- 24/7 situational awareness and crisis monitoring of critical infrastructure
- Shares threat information in order to reduce risk, prevent damage, and enable rapid recovery of critical infrastructure assets
- The NICC and the NCCIC are co-located to facilitate collaboration
- www.dhs.gov/national-infrastructure-coordinating-center

Homeland Security

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

Chemical Facility Anti-Terrorism Standards (CFATS)

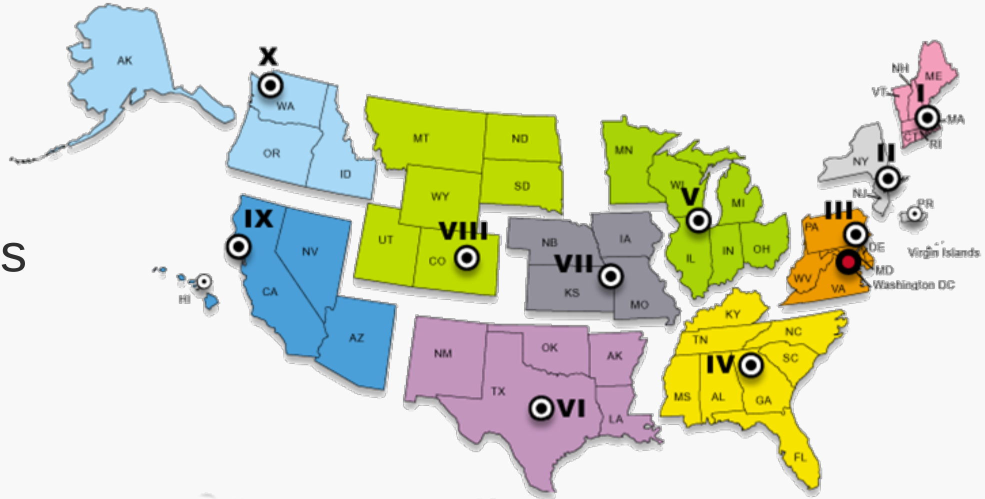
The CFATS regulation along with the Appendix A list of chemicals of interest can be found in 6 CFR Part 27.

- In 2007, Congress authorized the Department to regulate security at "high-risk" chemical facilities
- Any facility that maintains on its premises certain chemicals above a specified quantity (as listed in Appendix A of the CFATS regulation) may be considered "high-risk" and **must** complete and submit an online survey, referred to as a Top-Screen
- CFATS follows a risk-based approach, allowing DHS to focus on high-risk chemical facilities in accordance with their specific level of risk

- **Does CFATS apply to you?** Find out more at www.dhs.gov/chemicalsecurity or by contacting the CFATS Help Desk, toll-free, 1-866-323-2957 or by email, csat@dhs.gov
- **General Inquiries:** Email CFATS@dhs.gov

Chemical Security Inspectors

- Chemical Security Inspectors (CSIs) are located in all 50 States
  - Organized into teams in each of the 10 Federal regions
  - More than 130 CSIs
- Conduct:
  - Authorization Inspections
  - Compliance Assistant Visits
  - Compliance Inspections
  - Stakeholder Outreach



- CSIs also attend meetings with Federal, State, local, and private industry members

Homeland Security