Homeland Security

The Partnership Quarterly

From the National Protection and Programs Directorate, Office of Infrastructure Protection

July 2014

The Partnership Quarterly includes critical infrastructure security and resilience articles, highlights cross-sector initiatives, and identifies training and exercise opportunities, new tools and resources.

We want to hear from you! To subscribe or submit story ideas, please email Sector.Partnership@hq.dhs.gov with *"The Partnership Quarterly"* in the email subject line. We hope that you find *The Partnership Quarterly* useful, informative and a means of sharing and communicating your activities to the larger critical infrastructure community.

In This Issue...

- ChicagoFIRST and Public-Private Collaboration
- Silver Shield – Nevada's Critical Infrastructure Program
- 2014 National Homeland Security Conference - Preparedness Partnerships for the Whole Community
- IP Conducts Overland Park Active Shooter Workshop
- DHS Supply Chain Security Workshops Receive High Ratings from Private Sector; More Planned through 2014
- Office of Infrastructure Protection's Emergency Services Sector Releases "Roadmap to Secure Voice and Data Systems"
- Project Jack Rabbit: The Benefits of Research and Technology Transfer through Successful Public-Private Partnership
- Featured Training and Resources
- Featured Topic: Actions to Improve Chemical Facility Safety and Security – A Shared Commitment
- Mission Spotlight: The Strategic Environment for Countering Improvised Explosive Devices (IEDs)
- Upcoming Events

Partnership Perspectives

ChicagoFIRST and Public-Private Collaboration

Interview with Brian Tishuk, Executive Director ChicagoFIRST

How and when was ChicagoFIRST formed, and what are your future goals?

ChicagoFIRST was formed in 2003 by 14 Chicago-based financial institutions and has become a leader in regional critical infrastructure partnership and collaboration. ChicagoFIRST provides a forum within which critical firms - predominantly, but not exclusively, financial - collaborate with one another and, as a group, with government at all levels, to promote the resilience of their individual firms through local, regional, and national relationships.

ChicagoFIRST recognizes that public and private collaboration is a vital component of critical infrastructure security and resilience, In 2010, ChicagoFIRST partnered with the City of Chicago's Office of Emergency Management to form a permanent emergency management and homeland security forum for public-private collaboration. ChicagoFIRST co-chairs this group, now called the Chicago Public/Private Task Force, and has led the way in developing platforms for information sharing, emergency operations collaboration, and credentialing with the city before, during, and after an emergency or major event. Since its inception, ChicagoFIRST has expanded to include other sectors, and is working to broaden its cross-sector membership. Looking forward, ChicagoFIRST intends to expand its regional public sector collaboration to additional counties within the Chicago area.

What is an example of a critical infrastructure challenge your stakeholders have recently faced, and what resources were you able to provide?

One of the key drivers behind the establishment of ChicagoFIRST was credentialing. During incidents, facilities may be closed off to the public, limiting the private sector's ability to assess damage, conduct repairs, and continue business operations. To set the stage, ChicagoFIRST proposed the establishment of a public-private partnership with the city of Chicago to address these issues to critical infrastructure, including credentialing, and in 2010, the Chicago Public/Private Task Force was formed. It includes city public safety agencies and local private sector partnerships, and is chaired jointly by the Chicago Office of Emergency Management and ChicagoFIRST.

The 2012 NATO Summit in Chicago clearly illustrated the need for a credentialing process. ChicagoFIRST took on the task of proposing and drafting credentialing protocols, which addressed issues including identity verification, vetting, and testing parameters. By taking the weight off the public sector's shoulders, ChicagoFIRST enabled the city to focus on developing the logistical and practical aspects of the process. This two-pronged approach ensured that both the public and private sector had ownership in the result.

In 2014, this credentialing system, called the Business Recovery Access Program (BRAP), was

successfully tested against the city's draft general order and is now being incorporated into Chicago's general exercise program. It took many years to get to this point, but by prioritizing the issue and assisting substantially in the program's development, ChicagoFIRST was able to both meet the needs of its constituents while increasing Chicago's resilience.

What is one of the biggest challenges that you face as a public-private partnership?

One of the challenges we've seen is how difficult it can be to institutionalize the processes and relationships that have been established with our public sector partners. Informal relationships are not a strong enough footing when disaster strikes or key stakeholders change jobs. As such, through the Chicago Public/Private Task Force, ChicagoFIRST has made great strides with local government in establishing day-to-day and incident information sharing, strategic planning, and credentialing.

In what ways has your membership in the Regional Consortium Coordinating Council (RC3) facilitated the work of ChicagoFIRST in your critical infrastructure and resilience efforts at the local and regional level?

Membership in RC3 pays dividends by providing insight into how other regional consortia and stakeholders have addressed protection and resilience challenges, as well as how other groups have established public/private partnerships. Through RC3, ChicagoFIRST learned about the limited success other entities have had with credentialing, helping us understand the scope of the problem and potential ways to approach it.

Through the RC3, ChicagoFIRST has also been able to collaborate with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), which provides perspective on how other areas and levels of government have addressed these issues.

What do you feel is the primary benefit to organizations of becoming a member of the RC3?

The primary benefit of membership in RC3 is the built-in relationship with DHS, in addition to other partnerships. This connection enabled us to coordinate with the Federal Government on Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. Through this partnership, we will also be able to collaborate on new issues as they arise.

Photo Above: ChicagoFIRST logo, provided by Mr.Tishuk.

Please click here to return to the top of The Partnership Quarterly

Silver Shield – Nevada's Critical Infrastructure Program

Interview with Irene Navis, Plans and Operations Coordinator, Office of Emergency Management and Homeland Security, Clark County Fire Department - Las Vegas, NV

Silver Shield is Nevada's Critical Infrastructure Protection (CIP) program, managed and operationally coordinated by the Metropolitan Las Vegas Police Department.

What exciting or innovative partnership programs or initiatives are you currently involved with?

In Nevada, we have developed Silver Shield, which is a comprehensive program that incorporates and implements the National Infrastructure Protection Plan's risk management framework into the program's overall objectives. It provides vulnerability and risk assessments, maintains an inventory of Nevada's critical physical facilities from all 16 sectors, updates Nevada's IP Gateway, and houses a critical infrastructure protection tool for first responders.

What exciting or innovative partnership programs or initiatives are you currently involved with?

In Nevada, we have developed Silver Shield, which is a comprehensive program that incorporates and implements the National Infrastructure Protection Plan's risk management framework into the program's overall objectives. It provides vulnerability and risk assessments, maintains an inventory of Nevada's critical physical facilities from all 16 sectors, updates Nevada's IP Gateway, and houses a critical infrastructure protection tool for first responders.

The program was initially formed to conduct physical security assessments for key sites, but has evolved to enable Nevada to identify, prioritize, and assess risks to critical infrastructure assets, systems, networks and functions. Silver Shield assists with risk mitigation to a wide range of public and private sector stakeholders, enhances private sector coordination, and shares information across public and private sectors. The program is funded through a DHS grant administered by the Metropolitan Las Vegas Police Dept.

How long have you been a member of the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) and what do you value most about your involvement?

I have been a member for approximately three and a half years. The SLTTGCC provides an opportunity to discuss common infrastructure protection, security and resilience issues with my peers from other communities, and enables me to share issues and effective practices I've come across with my state, local, tribal, and territorial colleagues. It also allows me to understand the bigger picture and how Nevada fits in the critical infrastructure community, with DHS and the nation as a whole. Through the SLTTGCC, we coordinate on cybersecurity and homeland security issues in general, and I can then leverage that knowledge in such a way that I can provide better resources to my state. My involvement also enables me to share my State's own best practices with my SLTTGCC colleagues.

What are some practical examples of ways that you have successfully shared information with DHS and your SLTTGCC colleagues?

I highlighted Silver Shield for the 2010 SLTTGCC-sponsored Critical Infrastructure and Key Resources Partnerships Report. I was also interviewed for the 2012 Region IX SLTTGCC study of State and local critical infrastructure protection programs, and have formally presented the Silver Shield program to DHS, SLTTGCC and Alliance Network members during a SLTTGCC Plenary. I actively participated in the 2012 DHS/IP sponsored Critical Infrastructure Owner and Operator Focus Group for FEMA Region IX held in Las Vegas.

My State is also in the process of submitting a request for a 2015 Regional Resiliency Assessment Program (RRAP) study that would examine the issue of wastewater reclamation, and I am hoping to share the results of that analysis [if chosen] with my colleagues in other western states for which water preservation and reclamation is a critical topic.

What do you consider to be the two most important critical infrastructure related issues/topics for your State at the present time?

The biggest issue would be the linkages between cyber and physical security. Another topic is how to best use our infrastructure resilience planning and training to be better prepared to respond to and recover from man-made or natural disasters.

Photo Above: Clark County, NV Fire Department logo, Provided by Ms. Navis.

To be featured in an upcoming Partnership Perspective section please email: sector.partnership@hq.dhs.gov.

Please click here to return to the top of The Partnership Quarterly

Quarterly Highlights

2014 National Homeland Security Conference - Preparedness Partnerships for the Whole Community

Held in Philadelphia, PA, May 19-21, 2014.

This year's annual National Homeland Security Conference (NHSC) brought together homeland security professionals, emergency managers and planners, public safety representatives from across disciplines, local, State, and Federal government leaders from the Urban Area Security Initiative regions and metropolitan areas, and subject matter experts from the private sector to share best practices among those charged with keeping our Nation safe.

The DHS Office of Infrastructure Protection (IP), Sector Outreach and Programs Division (SOPD), led the very successful and well-received Preparedness Partnerships for the Whole Community track as one of ten offered at the conference. Session highlights included a panel discussion on the recently released Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience, both of which aim to strengthen the security and resilience of our Nation's critical infrastructure against evolving threats and hazards. The tenets of EO 13636 and PPD-21 provided key foundational pieces for the updated National Infrastructure Protection Plan with a Call to Action for implementing the risk management framework.

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) facilitated a session that offered participants the opportunity to learn more about the council's Regional Landscape Reports series. Those reports have been conducted to provide an overview of the progress, successes and challenges to the critical infrastructure security and resilience mission. In their presentation, Council members noted that State and local critical infrastructure programs are actively identifying critical infrastructure and leading assessments, as well as actively partnering and sharing information with private industry owners and operators.

During its presentation, the Regional Consortium Coordinating Council (RC3) provided lessons learned and best practices, to include the necessity of first identifying the critical need for the community or regional public-private partnerships, and establishing such partnerships independent of disruptive incidents. The RC3 also noted that development is underway on sector-specific working groups,

committees, and leadership to direct efforts within their area of jurisdiction, including sharing information on threats and incidents.

Other topics of interest included a panel addressing the State and local first responder community, strengthening the partnership approach, and ways Protective Security Advisors (PSAs) can leverage Regional Resiliency Assessment Programs to focus local stakeholders on the regional perspective. Panelists included DHS Senior Officials and program managers, State and local government partners, and private sector subject matter experts, contributing to well-rounded discussions from varying perspectives with active participation from the attendees.

Secretary Jeh Johnson addressed nearly 1,000 attendees during his keynote remarks at the conference. To learn from and adapt to evolving threats and hazards, Secretary Johnson highlighted the importance of continuing critical partnerships with State and local governments, as well as first responders, to strengthen and enhance security. Caitlin Durkovich, Assistant Secretary for Infrastructure Protection underscored the value IP's programs provide in support of the Nation's first responders, including information sharing through TRIPwire and HSIN-CI, close partnerships with local governments, and the work that the Protective Security Coordination Division provides through ongoing assessments, tools, and training.

Additional information regarding the 2014 NHSC, including the presentations from this and other tracks, can be found at: http://nationaluasi.com.

Please click here to return to the top of The Partnership Quarterly

IP Conducts Overland Park Active Shooter Workshop

Members of the Office of Infrastructure Protection (IP) have crisscrossed the country, bringing the cross-sector Active Shooter Workshop Series to communities eager to learn more about how to prepare for, and respond to, an active shooter situation. Of the nearly 100 workshops conducted since the program began in 2011, a few cities have been visited twice. In February 2012, IP held a workshop in Overland Park, Kansas at the Johnson County Community College, and recently held a workshop on May 30, 2014 at the Jewish Community Center, at the very site where a gunman killed two people just six weeks prior. During the incident, the gunman opened fire in the center's parking lot, killing a grandfather and his grandson, before going to the nearby Village Shalom senior care facility and killing a third victim, a woman visiting her mother. Following the shooting, IP contacted the Jewish Federation of Greater Kansas City, and coordinated the workshop at the Jewish Community Center.

Active Shooter Workshops include facilitated discussions and presentations from law enforcement and behavioral subject matter experts. The workshop on May 30 featured Lieutenant Colonel Simon Happer, Overland Park's Deputy Police Chief, as a guest speaker. While he could not discuss specifics of the April 13 shooting as the investigation is still ongoing, Lieutenant Colonel Happer detailed his department's active shooter program. IP's Ann Ratliff, along with workshop facilitators, delivered a thorough curriculum, including an historical perspective on active shooters, the typical law enforcement response, how to plan for an active shooter, the immediate actions to take if confronted with an active shooter, and emergency planning. The audience of nearly 150, which included faith-based and business leaders, "were extremely engaged," said Ratliff. "They were very responsive to our presentation and their questions were specific and insightful."

If you are interested in future workshops, please contact ASworkshop@hq.dhs.gov. For the complete

listing of DHS Active Shooter resources, please visit the Active Shooter Preparedness Webpage at www.dhs.gov/activeshooter.

Please click here to return to the top of The Partnership Quarterly

DHS Supply Chain Security Workshops Receive High Ratings from Private Sector; More Planned through 2014

In Spring 2014, the Office of Infrastructure Protection's Critical Manufacturing Sector organized Nation-wide Supply Chain Security Workshops. These day-long workshops were free to attend and designed to increase resilience and focus risk management efforts on supply chain security. The five workshops were held in Houston, Chicago, Philadelphia, Seattle, and Los Angeles.

Recognizing that the security of the global supply chain is vital to the Nation's welfare, these workshops reinforced the President's message of the importance of supply chain security contained in the 2012 *National Strategy for Global Supply Chain Security*. Topics covered both physical and cyber security concerns, and included: best practices in global supply chain security; Customs-Trade Partnership Against Terrorism (C-TPAT); intellectual property rights; intel briefs; the cyber threat landscape; a cyber framework for improving critical infrastructure; supply chain resilience through optimization; and, the recently released Executive Order 13659: *Streamlining the Export/Import Process for America's Businesses*. The workshops provided a unique opportunity for those interested in providing input to DHS on improving the supply chain management process through enhanced trade facilitation.

The audience for the Supply Chain Security Workshops included corporate and facility security professionals from the private and public sectors, supply chain security professionals, owners and operators, and government representatives with supply chain security responsibilities. Each workshop accommodated up to 100 people, and was promoted across all 16 Critical Infrastructure Sectors.

Participants committed to encouraging their organizations to incorporate information from the workshops into their security practices, as well as to share information from the workshops across their organization. Participants also said they would like to attend future workshops, and that the workshops were well structured, well organized, and included the right mix of topics, people, and training.

Building on the success of these workshops, DHS is planning to continue the Supply Chain Security Workshop series through 2014 and beyond by partnering with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) to leverage the members' understanding of supply chain challenges and potential solutions unique to State, local, tribal, and territorial governments.

Four to six new workshop locations are being planned in locations vital to supply chain security, and will be coordinated by members of the SLTTGCC from within these communities. One area of focus for upcoming workshops will be to help meet the supply chain security and resilience needs of cities with substantial cross-border traffic. A goal of each workshop will be to develop community-based activities that can enhance supply chain security and resilience, both locally and as a model for more broad national applications. Lessons learned and a best practices compendium will be developed for the Nation, and the efforts will be buttressed by the addition of Supply Chain Security tabletop exercises that can be used by partners on their own.

If you have any questions or comments about past or upcoming worlshops, or would like to see a workshop in your city, contact the Cross-Sector Supply Chain Working Group at CSSCWG@hq.dhs.gov.

Please click here to return to the top of The Partnership Quarterly

Office of Infrastructure Protection's Emergency Services Sector Releases "Roadmap to Secure Voice and Data Systems"

The Office of Infrastructure Protection, as the Emergency Services Sector-Specific Agency, is pleased to announce the release of the *Emergency Services Sector Roadmap to Secure Voice and Data Systems*. The Roadmap is a collection of cyber risk response strategies that address the cyber risks identified in the 2012 *Emergency* Services Sector Cyber Risk Assessment (ESS-CRA) completed under the *National Infrastructure Protection Plan* framework and is now available to emergency services personnel on the HSIN-ES and HSIN-CI Websites.

The Roadmap identifies and outlines several proposed risk mitigation measures, including response justification, application to discipline, implementation barriers, and suggestions for improvement. As in all other critical infrastructure sectors, the Emergency Services Sector (ESS), continues to adapt to a greater reliance upon digital technologies and other emerging protective program measures to manage cyber critical infrastructure risk, and enhance security and resilience.

Given public safety resource constraints, the Cybersecurity and Risk Management Approach efficiently and effectively provided a low-cost means for ESS subject matter experts to leverage and capitalize on their ESS-CRAs by identifying common and shared cyber risks across the sector, understanding what cyber infrastructure exists in the sector, and how it strategically supports public safety missions across the sector community. The March 2014 release of the Roadmap is the next step in ensuring that Federal resources are applied where they offer the most benefit for mitigating risk, limiting vulnerabilities, and minimizing the consequences of attacks and other incidents while encouraging a similar risk-based allocation of resources within State, local, tribal, and territorial entities, and the private sector.

Through the collaborative efforts of the U.S. Department of Homeland Security's Sector Outreach and Program Division and the Cyber Security and Communication's Industry Engagement and Resilience Branch within the Emergency Services Sector Cyber Working Group, seven cyber risk scenarios were developed and applied across multiple ESS disciplines. Threats, vulnerabilities, and consequences inherent to these ESS cyber risk scenarios were evaluated and an aggregate ESS risk profile was created. The Roadmap is a living document and the result of a public and private collaboration effort for the good of our Nation. The ESS Cyber Working Group will continue to assess the ESS-CRA and the Roadmap on a regular basis to consider including additional guidance covering emerging cyber risks, cyber incident trends, and other cybersecurity issues.

For more information, contact the Emergency Services Sector: ESSTeam@hq.dhs.gov.

Please click here to return to the top of The Partnership Quarterly

Project Jack Rabbit: The Benefits of Research and Technology Transfer

through Successful Public-Private Partnership

Project Jack Rabbit was the result of Congressional concern over 90-ton railcars filled with chlorine and other toxic chemicals, which pass through metropolitan areas approximately 30,000 times per year. First begun in 2009, *Project Jack Rabbit* is a series of chemical-release field trials that help government and industry better understand the behavior and consequences of large-scale hazardous chemical releases; and develop critical data necessary to enable risk reduction, mitigation, and physical/industrial cost avoidance. Data and findings from the project are improving hazard prediction modeling, emergency response and training, national preparedness, mitigation strategies, and infrastructure resilience. *Project Jack Rabbit* was recognized with an Excellence in Technology Transfer award in late 2013.

Chlorine trial release Stage 1 – after one second (DHS Photo)

Chlorine trial release Stage 2 Dispersion – after 10 minutes (DHS photo)

Jack Rabbit I Findings

Jack Rabbit I was a series of ten, one- and two-ton chlorine and ammonia field release trials intended to address data gaps for large-scale, hazardous chemical release disasters. The test enabled updated/validated chemical release/reaction modeling to support novel risk miti/gation strategies and enhancements in emergency response training for potential accidents or terrorist attacks on chemical storage tanks or railcars.

The team of public and private sector chemical scientists, chemical engineers, and transportation/manufacturing experts determined that emergency response protocols should be updated to address the persistent low, fog-like initial dispersion of chlorine and ammonia, chemical reactivity with the environment, and spontaneous explosive chlorine plumes. Based on new modeling, trial results highlighted the need to update emergency response guidelines to include chemical suit protection assumptions, surrounding community shelter-in-place, or evacuation protocols. Field test data from a parallel TSA/FBI project considered improvements in current tank rail cars' puncture resistant/crash worthiness design that did not exceed railroad track or highway weight limitations.

Jack Rabbit II

Jack Rabbit II expands and continues studies of *Jack Rabbit I* until 2018. Chlorine field releases from 5 to 20 tons consistent with actual potential releases are planned, providing data for scenarios that have never been investigated or experimentally observed. Data collection on the release source, exposure effects on equipment and infrastructure, urban impact via a mock urban test-bed, and environmental chemical absorption (ground, trees, wind, and managing water reactivity) will be considered. Based on Jack Rabbit I trials, scientific interest has also expanded to include Canadian chemical scientists and engineers in upcoming trials.

Excellence in Technology Transfer through Public/Private Partnership

2013 Awardees for Excellence in Technology Transfer - From left to right: Nohemi Zerbi, Shannon Fox, Adolfo Negron, Jack Aherne, and Patricia McKenney (not shown)

Following the first field trials, workshops bringing together over 150 emergency services, response, and planning representatives were held at the U.S. Army's Edgewood Chemical Biological Center in Edgewood, MD and the Association of American Railroads in Washington, D.C. Participants viewed test videos and discussed the implications to existing protocols for chlorine and ammonia releases, with all concurring that a novel approach was needed to transition the critical findings to private sector stakeholders. Working groups were established to develop a communications strategy. As a result of this effort, *Jack Rabbit* technology and knowledge products were transferred through four major trade associations representing hundreds of industrial members to include: The Chlorine Institute, the Ammonia Safety and Training Institute, The Fertilizer Institute, and the Association of American Railroads. The trade associations shared the findings through industry presentations, national-level emergency responder training, and field test data distribution.

The Mid-Atlantic Regional and National Federal Laboratory Consortium Award for Excellence in Technology Transfer was awarded to six chemical engineers, scientists, and program managers from the Office of Infrastructure Protection's Chemical Sector-Specific Agency, the Science and Technology Chemical Security Analysis Center (CSAC), the Transportation Security Administration, and the U.S. Army Dugway Proving Ground for their efforts to establish a Web-based data repository; modeling data and methodologies; training products from Project Jack Rabbit for the private sector; and novel risk mitigation strategies for the chemical, railroad, and emergency response industries.

The *Jack Rabbit* program successfully demonstrates a public-private partnership approach where several DHS directorates and other Federal agencies continue to work in unison with the private sector to further our national goals for the security and resilience of critical infrastructure. CSAC is currently seeking additional collaboration and stakeholder involvement to expand the test program through support, partnerships, and direct participation in the planning and field trials. For more information on Project Jack Rabbit, contact: ChemicalSector@hq.dhs.gov or Jack.Rabbit@st.dhs.gov.

Why Are Ammonia and Chlorine Important to You and Your Sector?

- They are essential to modern day life for health, safety, nutrition, security, transportation, lifestyle, and high-tech innovation
- Ammonia supports agriculture for fertilizer/crop protection product manufacturing
- Ammonia is used for refrigeration, explosives, chemical manufacturing, and consumer cleaning/disinfectant products.
- Chlorine is a $46 billion industry and a key component in over half of all industrial chemical processes to include pharmaceuticals and the manufacturing of plastics, paper, medical devices, automobiles, computers, aircraft parts, and textiles. (Source: U.S. Chemical Industry Statistical Handbook, American Chemistry Council)

Please click here to return to the top of The Partnership Quarterly

Featured Training and Resources

IS-912: Retail Security Awareness: Understanding the Hidden Hazards

The purpose of this course is to make persons involved in commercial retail operations aware of the actions they can take to identify and report suspicious purchases or thefts of products that actors could use in terrorist or other criminal activities. To achieve this goal, the course provides an overview of prevention steps aimed at identifying and monitoring high-risk inventory products and reporting suspicious activities to law enforcement agencies. This course is designed for retail managers, loss prevention specialists, risk management specialists, product managers, sales associates, and others involved in retail operations. The course can be accessed here.

General training inquiries should be directed to: IP_Education@hq.dhs.gov

HSIN Connect Tool Provides Webinar and Information Sharing Solutions

Homeland Security Information Network (HSIN) Connect utilizes the Adobe Connect Web-conferencing platform for free Critical Infrastructure mission-related webinars. With Connect, you can easily create interactive, virtual forums to reach remote stakeholders anytime, anywhere. Features of the tool include access management, built-in analytics, recording, VoIP, screen and video sharing, and live chat and polling.

The benefits of HSIN Connect go beyond just Webinars; these tools and features can be leveraged to solve more unique information sharing challenges like online training, on-demand videos, file sharing, team spaces, event registration, campaign tracking and more.

While anyone can participate in a HSIN Connect meeting, you must have a HSIN account to host a webinar or content. To request a HSIN-CI account, contact HSINCI@hq.dhs.gov with your name, e-mail address, organization, and the sector with which you are aligned.

Please click here to return to the top of The Partnership Quarterly

Featured Topic: Actions to Improve Chemical Facility Safety and Security – A Shared Commitment

Report on Executive Order 13650

On August 1, 2013, the President issued Executive Order (EO) 13650 - Improving Chemical Facility Safety and Security - to enhance the safety and security of chemical facilities and reduce the risks of hazardous chemicals to facility workers and operators, communities, and responders. Chemicals and the facilities that manufacture, store, distribute and use them are essential to our economy and livelihood, but the handling and storage of chemicals can present a risk that must be addressed.

The Federal Interagency Working Group organized to implement the EO has taken critical steps in bringing together Federal regulatory representatives and stakeholders with a vested interest in reducing the risks associated with the handling and storage of chemicals. These efforts represent a shared concern among those with a stake in chemical facility safety and security: facility owners and operators; Federal, State, local, tribal, and territorial governments; regional entities; nonprofit organizations; facility workers; first responders; environmental justice and local environmental organizations; and communities.

The release of the status report to the President on June 6, entitled *Actions to Improve Chemical Facility Safety and Security – A Shared Commitment*, summarizes the Working Group's progress, focusing on

actions to date, findings and lessons learned, challenges, and short and long-term priority actions. These priority actions, captured in a consolidated action plan, based on the information collected by the Working Group, focus on five specific thematic areas:

- Strengthen Community Planning and Preparedness
- Enhance Federal Operational Coordination
- Improve Data Management
- Modernize Policies and Regulation
- Incorporate Stakeholder Feedback and Develop Best Practices

This report is a milestone, not an endpoint. While the report describes many activities already underway to improve chemical facility safety and security, it also makes clear that much additional work is necessary to implement the consolidated action plan - an effort that will be completed over time and require the collective efforts of all of those with a stake in chemical facility safety and security.

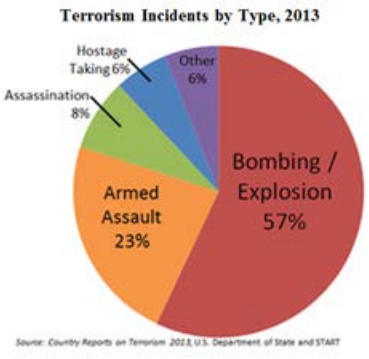
The report is the result of a Federal interagency working group led by the Environmental Protection Agency, the Department of Labor, and the Department of Homeland Security, and includes representation of other departments and agencies, such as Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Department of Agriculture, and the Department of Transportation, all of whom are involved in the oversight of chemical facility safety and security.

You can read a fact sheet about the report or view the full report.

Please click here to return to the top of The Partnership Quarterly

Mission Spotlight: The Strategic Environment for Countering Improvised Explosive Devices (IEDs)

From IP's Office for Bombing Prevention



In 2013, more than half of all terrorism incidents occurring world-wide involved the use of IEDs, more than any other tactic including armed assault (active shooters). Threats are becoming increasingly sophisticated – from the 2001 Richard Reed's shoe bomb, to the 2009 Christmas Day underwear bomb, to the 2010 Cargo Plane plot with IEDs concealed in printer toner cartridges, and now new non-detectible non-metallic devices. As we take measures to counter threats, adversaries are evolving their tactics through observation, trial and error, and exchanges of information. The IED and the bomber combine to make a "smart bomb" that can select its target, deliver its payload with precision timing and accuracy, and make mid-course adjustments based on the environment – presenting an extremely difficult challenge in preventing attacks. The Administration and Intelligence Community have stated that, due to the ready accessibility of materials and know-how to construct IEDs, IEDs are likely to remain the tool of choice into the foreseeable future.

Domestically, the 2013 Boston Marathon bombings serve as a reminder that IEDs are not just a problem that are limited to foreign shores or the war theater. In fact, IEDs remain one of the most accessible

weapons available to terrorists and criminals to damage critical infrastructure and inflict casualties here at home. IEDs are also a significant concern for our State and local partners. In their 2012 and 2013 Threat and Hazard Identification and Risk Assessments (THIRA), 90 percent of Urban Areas Security Initiative locations (UASIs) and 71 percent of States in 2012, and 81 percent of UASIs and 71 percent of States in 2013 indicated that IEDs were a hazard of concern – more than any other man-made or natural hazard. The technical know-how and materials to construct these deadly weapons are readily available in our stores and over the internet. Extremist literature, such as Inspire, not only provides the knowledge but also calls untold numbers of disaffected individuals, including persons within our own borders, to action. As demonstrated through Boston, people are reading this material, and the tactics discussed are actually being used within our own borders, by those with intent to kill, maim, or strike fear into the Nation. The latest edition of Inspire provides instructions for constructing deadly VBIEDs and provides recommendations for specific targets across the country.

The National Policy for Countering IEDs, the Office for Bombing Prevention, and You

The National Policy for Countering IEDs, articulated through Presidential Policy Directive 17, calls for a whole-of-government and all-of-Nation approach to preventing attacks before they become imminent. The policy acknowledges preventing attacks is not strictly the role of the Federal government, nor of our partners in State and local law enforcement. It specifically recognizes the role of the private sector as critical to successful implementation of the strategy. The fact is preventing attacks happens in our communities, in our neighborhoods, and in our store- and business-fronts, across the country, every day. Preventing attacks requires you. Enter the Office for Bombing Prevention. Our 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. We are an enabling organization that exists to assist our partners in the public and private sectors in their efforts to build their capabilities to counter the IED threat.

For more information about the Office for Bombing Prevention's information and resource sharing, capability analysis and planning support, and counter-IED training and awareness programs, products, and services, ask your DHS or non-DHS Sector Specific Agency or your local Protective Security Advisor for a copy of our Counter-IED Resources Guide, or contact OBP@dhs.gov.

Please click here to return to the top of The Partnership Quarterly

Upcoming Events

Chemical Security Summit: Baltimore, MD, July 22-24

The National Protection and Programs Directorate / Office of Infrastructure Protection (NPPD/IP) and the Chemical Sector Coordinating Council (CSCC) are co-sponsoring the eighth Annual Chemical Sector Security Summit. The Summit is scheduled for Tuesday, July 22, 2014 through Thursday, July 24, 2014 in Baltimore, MD.

This much anticipated event is an excellent opportunity to gain a better understanding of chemical security programs and regulations, to discuss cyber trends and tools, and to foster public/private dialogue. This year's speakers and session topics will provide a wealth of information and resources to enhance your security efforts. Session topics include Improving Chemical Facility Safety and Security EO 13650, Chemical Facility Anti-Terrorism Standards (CFATS) updates, International Trends in Chemical Security, and Transportation (Trucking, Rail and Pipelines), and voluntary programs. Summit participation enhances the protection and resilience of the Nation's fixed critical infrastructure, and emphasizes the Department's commitment to bilateral information sharing—essential elements of the DHS mission and core responsibilities.

For more information on this event, please visit www.dhs.gov/chemical-security-summit.

Surveillance Detection for Law Enforcement and Security Professionals

This course provides the participant instruction on how to detect hostile surveillance by exploring surveillance techniques, tactics, and procedures from a hostile perspective. This course is three days long and is designed for law enforcement and public/private sector security staff. Locations and points of contact are below:

- July 28: Parkersburg, WV. Ken Ullom, Kenneth.ullom@dhs.gov
- August 4: Ft. Bragg, NC. CPT Steven Breen, steven.j.breen@soc.mil
- August 5: Chicago, IL. John Busch, john.busch@hq.dhs.gov
- August 12: Washington, DC. David Riedman, davidr@downtowndc.org
- August 19: Nashville, TN Eric Bollinger, eric.bollinger@tsa.dhs.gov
- August 19: Atlantic City, NJ Michael Smith, Michael.smith@ohsp.state.nj.us

IED Search Procedures Workshop

This workshop increases IED awareness and educates participants on bombing prevention measures and planning protocols to detect IEDs by reviewing specific search techniques. This workshop builds knowledge of counter-IED principles and techniques among first responders and public/private sector security partners tasked with IED search and response protocols. This eight-hour workshop can accommodate 40 participants. Locations and points of contact are below:

- July 31: Parkersburg, WV Ken Ullom, Kenneth.ullom@dhs.gov

Vehicle-Borne IED (VBIED) Detection Course

This course improves the participant's ability to successfully inspect for, detect, identify, and respond to a VBIED. Instruction covers the VBIED threat, explosive effects, IEDs, and vehicle inspections, enabling participants to detect, deter, and protect against the illicit use of explosives. The course is designed for first responders and public/private sector security staff tasked with inspecting vehicles for explosives, dangerous goods, or any contraband. This eight-hour course can accommodate 20 participants. Locations and points of contact are below:

- August 1: Parkersburg, WV Ken Ullom, Kenneth.ullom@dhs.gov
- August 6, Orlando, FL Scott Langford, scott.langford@disney.com
- August 7, Orlando, FL Scott Langford, scott.langford@disney.com
- August 20, Springfield, VT Gabe Palazzi, Gabriel.palazzi@dhs.gov
- August 27, Houston TX Patrick Seeba, pseeba@hscsd.org

Bomb-Making Materials Awareness Program (BMAP) Training

BMAP is an outreach initiative, developed in partnership with the Federal Bureau of Investigation (FBI), to increase public and private sector awareness of homemade explosives (HME) by promoting private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of explosive precursor chemicals, explosive powders, and components commonly used in IEDs. BMAP training is designed for first responders responsible for outreach to build knowledge of IED threats, HMEs, and bomb-making materials. The course also provides guidance and materials to help participants conduct outreach to industries and businesses within their jurisdiction in order to strengthen prevention opportunities by building a network of vigilant and informed private sector partners who serve as the Nation's counter-IED "eyes-and-ears". Locations and points of contact are below:

- August 7, Washington DC Kelly Wilson, Kelly.wilson@hq.dhs.gov

IED Counterterrorism Workshop

This workshop enhances the participant's understanding of the IED threat, surveillance detection methods, and soft target awareness. The workshop also covers awareness and prevention measures, as well as, collaborative information-sharing resources to enable first responders, and critical infrastructure owners, operators, and security staff to deter, prevent, detect, and protect against the illicit and terrorist use of explosives in the United States. This eight-hour workshop can accommodate 250 participants. Locations and points of contact are below:

- August 19, Springfield, VT Gabe Palazzi, Gabriel.palazzi@dhs.gov

IED Awareness/Bomb Threat Management Workshop

This workshop improves the participant's ability to manage IED threats by highlighting specific safety precautions associated with explosive incidents and bomb threats. The workshop reinforces an integrated approach that combines training, planning, and risk assessment to maximize available resources for bomb threat management. This workshop is four hours long and is designed for facility owners, operators, and security staff. Locations and points of contact are below:

- August 20, Baltimore, MD Ray Hanna, ray.hanna@hq.dhs.gov
- August 27, Columbus, OH Steve Saltsman, ssaltsman@columbus.gov

Please click here to return to the top of The Partnership Quarterly

---

November is Critical Infrastructure Security and Resilience Month

Now is the time to start planning how your organization will contribute to building awareness and understanding of the importance of critical infrastructure to America's national security and economic prosperity as well as reaffirming the commitment to keep our critical infrastructure and our communities safe and secure. Look for more information early this Fall.