NIPP Newsletter

Homeland Security

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 36: AUGUST/SEPTEMBER 2008

Topics in this Issue

Upcoming NIPP CIKR Events

- **SEPTEMBER 21-25**
  National Association of State EMS Officials 2008 Annual Meeting, Tacoma, WA
- **OCTOBER 9**
  Federal Senior Leadership Council Meeting, Arlington, VA
- **OCTOBER 19-23**
  Association of State Drinking Water Administrators Annual Conference, Colorado Springs, CO

NIPP-Related Activities and Events

2008 Chemical Sector Security Summit

The National Infrastructure Protection Plan (NIPP) Sector Partnership Model provides a mechanism for government and private-sector partners to network and share information. One example of this is the 2008 Chemical Sector Security Summit, co-sponsored by the Chemical Sector-Specific Agency within the Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) and the Chemical Sector Coordinating Council (CSCC).

A three-day event held in Bethesda, MD on July 21–23, the Summit provided a forum for attendees to exchange information and ideas as well as network with other security professionals. According to Timothy Scott, Chair of the CSCC, "The Security Summit was an excellent example of the continuously improving partnership between DHS and the private sector. The information and topics were timely, and the speakers were experts in their areas."

Participation in this year's Summit matched attendance levels of the first Summit, held in June 2007, with more than 400 attendees representing a broad range of the chemical stakeholder community, including:

- corporate and facility security personnel;
- environmental, health, and safety personnel;
- chemical transportation and distribution personnel;
- congressional staff; and
- Federal, state and local government officials representing a variety of critical infrastructure and key resources (CIKR) sectors.

Almost 75% of the participants were from the private sector with the remainder from Federal, State, and local governments.

The Summit allowed chemical industry partners the opportunity to ask specific questions about the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory process and gain insight into the role of different agencies and departments involved in the many facets of chemical security. Topics generating the most interest from participants included Risk-Based Performance Standards; programs created to safeguard sensitive information; and the CFATS inspection and compliance process. Smaller breakout sessions addressed topics in detail, including State and local issues, cybersecurity, and freight rail security, and provided opportunities to attend several software demonstrations.

DHS Infrastructure Security Compliance Division (ISCD) staff members were on-hand to explain the procedure for entering facility data into the Security Vulnerability Assessment (SVA) tool. DHS hopes this tool will facilitate submission of security

(more)

and vulnerability data for facilities subject to preliminary CFATS regulations. Also enjoying its official launch was the Web-Based Chemical Security Awareness Training Program. This is a voluntary program using instruction modules that simulate real-world scenarios for interactive learning. It is designed to increase security awareness in chemical facilities nationwide with the potential for reaching 400,000 employees directly involved in the manufacturing, transportation, and storage of chemicals. For more information about this program or to request access, send an email to ChemicalSector@dhs.gov.

Other highlights of the 2008 Summit included a Keynote Address by DHS National Protection and Programs Directorate (NPPD) Deputy Under Secretary Scott Charbo and a Luncheon Address by Assistant Secretary for Infrastructure Protection Robert B. Stephan. Both senior DHS officials highlighted the successful voluntary programs created as a result of the public-private partnership and encouraged participants to continue their efforts in the future. In closing the Summit, Assistant Secretary Stephan advised the audience to continue supporting the partnership to demonstrate the many benefits that can be realized through a voluntary program that complements a regulatory framework.

DHS Prepares for National Cyber Security Awareness Month in October

October 2008 marks the fifth anniversary of National Cyber Security Awareness Month. The Department of Homeland Security (DHS) is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. As called for in The National Strategy to Secure Cyberspace, *Priority III,* DHS is working with appropriate Federal, State, and local entities and private sector organizations to "promote a comprehensive national awareness campaign, to empower all Americans – businesses, the general workforce, and the general population – to secure their own parts of cyberspace."

DHS leaders kick off the Month at an October 2nd event with the National Cyber Security Alliance. Senior DHS leaders will be traveling around the country speaking to audiences about the importance of cybersecurity and the Department's accomplishments and goals. They will also raise awareness about cybersecurity, the importance of enterprise risk management, the role of partnerships in safeguarding the Nation's cyber infrastructure, as well as urge all Americans to safeguard their networks and computers at home, school, and in the office.

Through the NIPP framework, DHS leads a comprehensive effort to improve the resiliency of our Nation's critical infrastructure by working with Federal, State, and local agencies, and the private sector. Critical infrastructure is increasingly interdependent with information technology systems and computer networks for essential operations. Therefore, preparing your customers, your employees, and your systems to be vigilant of the cyber threat is essential to reducing cyber risks. Together, these activities will also enhance strong public-private relationships and facilitate coordination within and across all 18 CIKR sectors.

We hope your organization will take part in National Cyber Security Awareness Month this October by re-committing your efforts to better secure your cyber assets, networks, and systems. Below are some practical cybersecurity activities your organization can implement to raise awareness:

- Educate yourself with tips and guides from www.StaySafeOnline.org. Email monthly reminders to employees to change their passwords.
- Reach out to your customers – through newsletters, email alerts, web sites, and billing statements – and promote your commitment to cybersecurity.
- Find cybersecurity posters on www.OnGuardOnline.gov and post them in work-rooms, hallways, bathrooms and other employee-gathering places. Print and post cybersecurity tips near your computer in a prominent location.
- Organize a brown bag lunch with a cybersecurity expert.
- Encourage employees to report any suspicious incident to your IT department or to DHS at www.US-CERT.gov.
- Create a separate section for cybersecurity tips on your organization's web site. Download online button and banners about phishing, identity theft, file-sharing, and other cybersecurity topics at www.OnGuardOnline.gov and place on your organization's home page.
- Subscribe to the National Cyber Alert System from US-CERT at www.US-CERT.gov.

Through the Alert System, you can receive timely information about current cybersecurity problems to protect home and office computers. This information includes weekly bulletins with summaries of new vulnerabilities, patch information when available, and tips on common security topics, such as privacy, email spam, and wireless protection.

Infrastructure Protection Office Holds First Web-based Seminar

Webinar aimed at educating DHS partners about links between NRF and NIPP

The DHS Office of Infrastructure Protection (IP) is hosting a series of Web-based seminars on different topics for its private sector and government partners. Based on the first of these events, which drew more than 300 participants on August 26, there is a keen level of interest. This seminar was designed to educate participants about the linkages between the Critical Infrastructure and Key Resources (CIKR) Support Annex of the National Response Framework (NRF) and the National Infrastructure Protection Plan (NIPP)—two documents used in responding to and preparing for disasters.

The initial seminar, entitled "Engaged Partnerships for Disaster Response," covered the roles of the public and private sector during disasters. "The ability of our Nation to prepare for, respond to, and recover from hurricanes, tornadoes, floods, or other natural disasters or terrorist attacks, depends on a strong, vibrant and sustained partnership between government and the private sector, which owns and operates the vast majority of our critical infrastructure," said featured speaker R. James Caverly, Director of the IP Partnership and Outreach Division. "The CIKR Annex to the new National Response Framework provides the essential roadmap for the engaged partnership."

The 2008 CIKR Learning Series continues through the fall, with additional seminars designed to provide CIKR owners and operators and other partners with current information about the tools, latest trends, issues and best practices in the infrastructure protection arena. The upcoming fall schedule includes:

- "Improvised Explosive Devices: Are You Ready?" – October 15, 2008, 1 p.m. - 2 p.m;
- "Bomb Threat Management" – October 24, 2008, 1 p.m. - 2 p.m.; and
- "Working with Regional Coalitions to Implement the National Infrastructure Protection Plan" – November 12, 2008.

More information about IP, the NIPP, and the Webinar series is available at:
http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm

Important News for the Sectors

Cyber Storm II Exercise Yields Significant Benefits

The Department of Homeland Security's National Cyber Security Division conducted the Nation's largest and most comprehensive cybersecurity exercise on March 10-14, 2008. The exercise simulated a coordinated, large-scale cyber attack on four of the Nation's critical infrastructure sectors – Chemical, Communications, Information Technology, and Transportation Systems (rail/pipeline). The participation of these sectors was coordinated through the Information Sharing and Analysis Centers, Sector Coordinating Councils, and Government Coordinating Councils.

The exercise engaged participants from 18 Federal departments and agencies, nine States, more than 40 private sector companies from within the U.S., and four international partners. Throughout the planning process, exercise planners from the public and private sector collaborated to design a comprehensive scenario that allowed participants to better understand the interdependencies of physical and cyber infrastructure and to achieve their individual organizations' goals to improve cybersecurity and cooperation during a crisis.

The scenario was based on organizational and sector exercise objectives drawn largely from existing security policies, vulnerability assessments, and risk profiles. Players were challenged to respond to diverse threat vectors including simulated significant Internet disruptions that impacted several top-level domains, thus making Internet access difficult and sometimes impossible. On top of that, players experienced a widespread telecommunications disruption that caused unreliable telephone service across the country.

Cyber Storm II highlighted the growing importance of cybersecurity to each of the Nation's critical infrastructure sectors. The exercise

(more)

strengthened the ability of participating organizations to prepare for, protect against, and respond to the effects of cyber attacks. For the Federal Government, Cyber Storm II exercised strategic incident response decision making and interagency coordination in accordance with the new National Response Framework and other national-level policies and procedures.

Since the conclusion of the exercise, players have been involved in a series of After Action Conferences to capture insights and findings. One of the biggest findings validated in the exercise was the importance of having established relationships within the cybersecurity, emergency response, and homeland security communities. The exercise also demonstrated that coordination and information sharing have significantly improved since Cyber Storm I through formalized processes taking maximum advantage of Sector Coordinating Councils, Government Coordinating Councils, and Information Sharing and Analysis Centers. These findings will be included in a complete After Action Report to be released later this year.

For more information about Cyber Storm II, please refer to the Cyber Storm II Web Page: http://www.dhs.gov/xprepresp/training/gc_1204738275985.shtm.

New PCII Program Materials Provide Additional Guidance for Government Partners

All recipients of Protected Critical Infrastructure Information (PCII) are responsible for ensuring that PCII is properly safeguarded. To assist Federal, State and local entities in their responsibility to properly implement the PCII Program, the PCII Program Office developed a series of informational materials to reinforce procedures explained in the PCII computer-based and instructor-led trainings. The PCII Program Best Practices Series helps PCII recipients understand the policy and procedural requirements necessary to receive, handle and safeguard PCII, by providing additional guidance on:

- Access, Dissemination and Use
- Categorical Inclusion
- Day-to-Day Operations
- Designee Roles and Responsibilities
- Officer Roles and Responsibilities
- Oversight and Compliance
- Self-Inspection Program

The Department of Homeland Security established the PCII Program and developed implementing regulations in accordance with the Critical Infrastructure Information (CII) Act of 2002. The PCII Program protects CII that owners and operators of critical infrastructure and key resources voluntarily share with the government. Information validated and marked as PCII is protected from disclosure under the Federal Freedom of Information Act (FOIA) and similar State and local disclosure laws, and from use in civil litigation. Additionally, PCII cannot be used as the basis for regulatory action.

Information regarding the submission process, access requirements, safeguarding procedures, and required PCII regulation statements is available on the PCII Program web site at www.dhs.gov/pcii.

Contact the PCII Program Office at pcii-info@dhs.gov or (202) 360-3023 to request a copy of the Best Practices Series or for more information on the PCII Program.

Maritime Security Risk Analysis Model Supports Risk Assessment and Resource Allocation

The U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) was rolled out in 2006 and is reviewed and improved annually. The model provides commanders at all levels – from Captains of the Port to senior DHS leaders – with risk information to support tactical, operational, and strategic decisions to strengthen infrastructure protection and reduce the risk of terrorism along the Nation's navigable waterways.

The complexity of the maritime domain presents a unique challenge and the Coast Guard needed a program that would address a vast array of diverse assets and systems. MSRAM is designed to identify, evaluate, and prioritize critical infrastructure, key resources, and high-consequence transits and events across sectors, using a common risk methodology, taxonomy, and metrics to measure security risk at the local, regional, and national levels.

(more)

Since 2006, MSRAM data have been used to identify those ports at highest risk to support the distribution of Port Security Grants. In some ports, sector staff work with requesters to pre-assess the impact of proposed grants, and use MSRAM to help local stakeholders craft more effective risk mitigation strategies to apply toward the Port-Wide Risk Mitigation Plans. Grant requests are then prioritized by the sector commander based on national priorities, cost-benefit analyses, and risk mitigation potential as determined by MSRAM.

For preparedness exercises mandated by the Maritime Transportation Security Act (MTSA), Coast Guard Headquarters staff use MSRAM data to focus resources on those facilities determined to be at greatest potential risk of terrorist attack. By focusing on high-risk facilities, as Congress intended, the number of affected facilities remains manageable and the Coast Guard avoids unintended consequences and undue burdens on industry.

Going forward, the Coast Guard will broaden MSRAM methodology to address the threat posed by the transfer of terrorists and terrorist materiel from foreign countries into the United States via its ports of entry, a challenge requiring multinational and multi-agency cooperation and collaboration. This program, called MSRAM PLUS, will support analysis of this aspect of the terrorist threat, beginning with overseas components in the commercial shipping system and following them into the United States.

MSRAM has proved to be less expensive and more expedient than other programs and, while it is currently designed to assess various kinds of attacks, the Coast Guard is working with DHS to develop an all-hazards model that will also assess risk from natural disasters. With a Homeland Security Risk Assessment Model (HSRAM) for the States, the methodology could be used department-wide to support the strategic missions of prevent, protect, respond, and recover.

Assessing risk and focusing resources effectively to support policy, strategy, regulations, forces, and local tactical actions is a daunting challenge that crosses all sectors and borders. Not surprisingly, the Coast Guard's success with MSRAM has drawn attention from many quarters, including 12 States and 5 other countries.

For more information about the MSRAM program, contact LCDR Brady Downs at Brady.C.Downs@uscg.mil, LT David Dixon at David.D.Dixon@uscg.mil, or Mr. Jeff Fuller at Jeff.Fuller@tbe.com.

U.S. Department of Defense Receives PCII Accreditation

The Protected Critical Infrastructure Information (PCII) Program recently accredited the Department of Defense (DoD) as part of an information-sharing partnership to enhance DoD's critical infrastructure information (CII) collection efforts.

Under the CII Act of 2002, information submitted voluntarily and validated as PCII is protected from public disclosure under the Federal Freedom of Information Act (FOIA) and similar State and local disclosure laws, and from use in civil litigation.

DoD is one of several Federal entities working with the PCII Program to integrate PCII protections into its data-collection processes, which will further enhance its information-sharing initiatives with the private sector.

The PCII Accreditation Program enables DoD to access CII it may not otherwise have for homeland security purposes. In addition to DoD, the Nuclear Regulatory Commission (NRC) and a component of the Department of Health and Human Services (HHS) are PCII-accredited. To date, more than 57 Federal, State and local entities have access to PCII through the PCII Accreditation Program. Illinois and South Dakota are the most recently accredited States.

Federal government entities interested in integrating PCII protections into their data collection efforts must first initiate the PCII accreditation process. Accreditation helps ensure government entities maintain stringent PCII safeguarding and handling requirements. The PCII Program encourages all government entities with information-collection needs to consider participating in the PCII Accreditation Program.

For more information, please contact the PCII Program Office at (202) 360-3023 or PCII-info@dhs.gov or visit www.dhs.gov/PCII.

> NIPP Resources Available for Security Partner Use

The free on-line NIPP training course is available at http://training.fema.gov/EMIWeb/IS/crslist.asp (enter course number IS-860). The NIPP trade show booth is also available for sector use. Please contact NIPP@dhs.gov for information on NIPP PMO participation and/or exhibition at an upcoming sector event or to schedule one of the growing cadre of trained speakers who can be deployed to sector events to speak on CIKR issues.

> Implementation Success Stories

The NIPP PMO continues to seek NIPP and/or SSP implementation success stories from the sectors to be shared with other security partners. Please submit any suggestions or brief write-ups to the NIPP PMO at NIPP@dhs.gov.

> NIPP Newsletter

The NIPP Newsletter is a product of the NIPP PMO and NIPP security partners are welcome to submit input. If you have any questions about the Newsletter or would like to submit information for inclusion in upcoming issues, please contact the NIPP PMO at NIPP@dhs.gov. Recipients of this newsletter are encouraged to disseminate it further to their security partners.