



Homeland
Security

NIPP NEWS

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 60: APRIL 2011

Critical Infrastructure Activities and Events

Spring Plenary Highlights Continued Collaboration Between SLTTGCC and IP

The State, Local, Tribal, and Territorial (SLTT) Government Coordinating Council (SLTTGCC) held its annual Spring Plenary in Seattle, Washington, on April 19–21, 2011. The Council helps to represent SLTT governments from across the country and works directly with the Office of Infrastructure Protection (IP) to develop national critical infrastructure protection and resilience policy and programs. The plenary provided an opportunity for the Council and IP to review IP's core programs, including the Protective Security Advisor program, Buffer Zone Protection Program, and the Automated Critical Asset Management System.



The plenary afforded Assistant Secretary Keil an opportunity to recognize Ulie Seal in front of the full Council, in appreciation for his dedicated efforts as the Chair of the SLTTGCC. His two-year term ends in June 2011.

Last November, the Council provided recommendations to improve 16 of IP's key programs that help SLTT governments advance the infrastructure protection mission. Noting the significance of the Council's recommendations in his opening remarks at the plenary, Assistant Secretary Keil said, "I see [these recommendations] serving as a blueprint for how IP can take the next step and deliver tailored programs that fit the needs of our critical infrastructure mission partners." IP program managers and Council members used the plenary to chart a specific course for implementing the Council's recommendations.

The 2011 plenary afforded IP an opportunity to introduce new programs and activities to Council members. IP provided an update on two new initiatives focused on regionalization and resilience. Through its Regionalization Initiative, IP will tailor its tools and programs to align more closely with the needs of its partners in the field. The SLTTGCC and IP's Regionalization Working Group will coordinate this effort in concert with the NIPP partnership.

The goal of the Resilience Initiative is to foster greater critical infrastructure resilience by identifying gaps in national resilience efforts and working with mission partners to determine how best to address those gaps. The Council has developed a draft report of State and local infrastructure resilience activities, with preliminary recommendations for IP on how to address the gaps that have emerged. The Council intends to publish this report later this summer.

"IP needs to get its programs out of Washington and into the field," Keil said. He added that IP will continue to work closely with the Council to extend the reach of its programs and tools to the regional requirements of IP's partners.

The path forward from the Spring Plenary includes a continuing dialogue on progress and effectiveness to ensure that IP's programs meet the needs of the partners charged with implementing protection and resilience programs across the country. This dialogue will take place through the Council's working groups, Webinars, and future plenary sessions.

For more information about the Council, visit <http://www.dhs.gov/slittgcc>.

Topics in this Issue

- > Spring Plenary Highlights Continued Collaboration Between SLTTGCC and IP
- > Japan Earthquake Under-scores the Relevance of NLE 11 Scenario
- > IP and FBI to Co-Host Regional Infrastructure Protection Symposia
- > Chemical Sector Makes a Case for Securing Industrial Control Systems

Japan Earthquake Underscores the Relevance of NLE 11 Scenario

The 9.0 magnitude earthquake that hit northern Japan on March 11, 2011 resulted in widespread destruction and loss of life. As of April 18th, the Japanese government reported an estimated 135,000 buildings destroyed or damaged; 13,116 people killed; 2,872 people injured; and 14,377 people missing. Approximately 206,400 evacuees are spread out among 2,300 shelters.

A large earthquake event in the United States is not without precedent; 2011 is the bicentennial anniversary of the 1811 New Madrid Seismic Zone (NMSZ) earthquake. Numerous studies have focused on a central U.S. earthquake in the NMSZ, involving the States of Alabama, Arkansas, Illinois, Indiana, Kentucky, Mississippi, Missouri, and Tennessee.

It is estimated that an NMSZ earthquake with a 7.7 magnitude could result in direct economic losses totaling nearly \$300 billion, and that indirect losses could be twice this amount, which would potentially result in the largest economic loss due to a natural disaster in U.S. history. The impact on critical infrastructure from such an event is expected to be substantial. Estimates indicate nearly 715,000 buildings would be damaged in the eight-state region. The human toll would be catastrophic as well, with an estimated 86,000 combined injuries and fatalities.

The National Level Exercise 2011 (NLE 11)

NLE 11 will help businesses; critical infrastructure owners and operators; Federal, State, and local government agencies; and others to prepare for a large-scale NMSZ earthquake. NLE 11 will focus on regional catastrophic response and recovery activities among all levels of government and private sector participants. The private sector has had extensive involvement in the design of NLE 11, through private sector working groups located in each of the States and through the national private sector working group, which includes 395 participants across 276 companies. As a subset of this group, critical infrastructure owners and operators have added credibility and validity to this exercise, with 176 participants representing 112 companies across 15 sectors.

A significant change in this year's NLE will be the full involvement of the private sector as part of the simulation cell during the exercise. This option allows sector-specific subject matter experts to review exercise plans and scenario input to ensure that they accurately reflect real-world private sector operations.

NLE 11 Tabletop Exercise

In addition to full-play opportunities for the private sector during the exercise, a self-directed, downloadable tabletop exercise and virtual engagement option will be available. The self-directed tabletop exercise allows organizations to participate in a scaled-down version of NLE 11 by providing all the required tools and information about the NMSZ earthquake in an electronic format that can be customized to suit an organization's needs. The virtual engagement option allows organizations and individuals to follow the flow of the exercise and consider the impacts on their own community and environment.

National Level Exercise 2011

WHEN:

May 16-19, 2011

WHO SHOULD PARTICIPATE:

Organizations with responsibilities in critical infrastructure protection, including Federal, State, local, and tribal government agencies; owners and operators; nonprofit agencies; academic institutions; nongovernmental organizations; and other critical infrastructure stakeholders, such as trade associations.

BENEFITS OF PARTICIPATING:

- Learn how to better prepare for an all-hazards event
- Build and foster relationships at the Federal, regional, State, local, and tribal levels
- Practice your business continuity plan
- Increase awareness of how to respond in an emergency
- Protect your bottom line—being prepared will result in less downtime and fewer lost employee work hours

UPCOMING MEETINGS:

The NLE 11 Exercise Calendar is continuously updated based on exercise planning and development outcomes. Currently the NLE 11 key dates are as follows:

- Great Central U.S. Shakeout April 28, 2011
- Functional Exercise TTX May 16-19, 2011
- National Recovery Seminar June 2011
- Recovery Exercise TTX September 20-22, 2011

QUESTIONS:

For more information about NLE 2011, contact:
private.sectorNLE@hq.dhs.gov

IP and FBI to Co-Host Regional Infrastructure Protection Symposia

The Office of Infrastructure Protection (IP) and the Federal Bureau of Investigation (FBI) will host five regional symposia in the summer of 2011 to collaborate more closely with critical infrastructure stakeholders across the Nation. The FBI and IP formalized an interagency partnership in 2009 to coordinate on activities that extend their reach into the local critical infrastructure community. The Joint Critical Infrastructure Partnership (JCIP) draws on the tremendous local resources available through public and private sector partners to reduce risk, promote awareness, and provide opportunities to enhance infrastructure protection and resilience at the local and regional levels.

The JCIP regional symposia will take place in Atlanta, GA; Chicago, IL; Houston, TX; Newark, NJ; and San Diego, CA. These events will provide a forum to exchange ideas at the local and regional levels and discuss infrastructure security and resilience initiatives. Attendees will include local and regional critical infrastructure owners and operators, trade association representatives, members of the 86 FBI InfraGard Chapters, representatives of the Alliance Networks established by the State, Local, Tribal, and Territorial Government

Coordinating Council, and local members of Sector Coordinating Councils. For regions not reached by the planned symposia, DHS and the FBI will offer additional outreach opportunities—such as information booths or sessions—at other events around the country.

Each symposium will include three core sessions to engage participants on IP partnerships, FBI InfraGard, and fusion centers. Additional topics may be added to highlight issues of importance to the specific region and relevant DHS and FBI activities and programs. JCIP will provide materials to increase awareness of infrastructure protection and resilience initiatives, including brochures, program fact sheets, and articles highlighting partner achievements across the Nation.

For more information about the JCIP Symposia, email Sector.Partnership@hq.dhs.gov. For more information about InfraGard, visit www.InfraGard.net.

Joint Critical Infrastructure Partnership

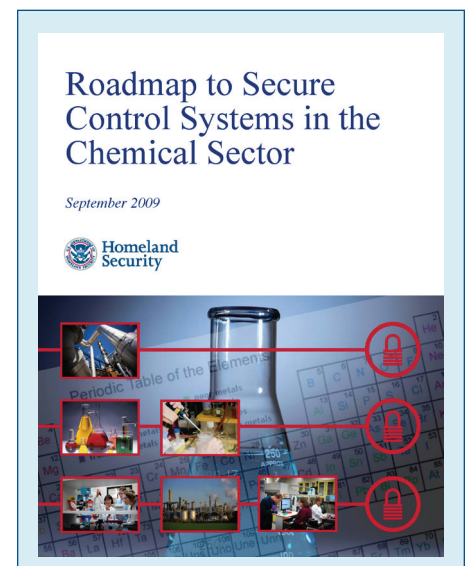
DHS ★ FBI – InfraGard



Chemical Sector Makes a Case for Securing Industrial Control Systems

In 2009, the chemical industry partnered with the Department of Homeland Security (DHS) to publish the *Roadmap to Secure Control Systems in the Chemical Sector* (Roadmap). This document provides a vision and supporting goals and objectives for improving the cybersecurity posture of Industrial Control Systems (ICS) within the sector. With a central emphasis on achieving objectives through public-private partnerships, the Roadmap calls for a comprehensive plan for improving the availability, security, reliability, and functionality of ICS by identifying key milestones over the next decade. The Chemical Sector-Specific Agency partnered with chemical industry owners and operators, the Chemical Sector Coordinating Council, and the National Cyber Security Division to form the Roadmap Implementation Working Group to address the milestones described in the document.

The proactive coordination of this effort proved to be timely. The emergence of Stuxnet, the first malware created specifically to target ICS, signaled a paradigm shift for the process control and automation industries. No longer are legacy control system environments isolated or invulnerable to information technology-specific threats. As news spread of this malware's impacts on ICS, securing the ICS environment became a priority for the Chemical Sector.



Launching the Roadmap Awareness Campaign

The working group identified milestone 1.1 of the Roadmap as the essential first step for implementation. This milestone specifically calls for the partnership to:

“Establish an industry-driven awareness effort to communicate information relating to the cybersecurity threats, vulnerabilities, and risks and the availability of accepted practices, tools, and training materials to the Chemical Sector.”

The working group collected extensive training and reference information to assist owners and operators in addressing ICS security. Roadmap awareness materials include the following:

- **Case for Action** – The campaign’s central document demonstrates the importance of taking action with the materials provided.
- **ICS Security Training Resource** – This guide lists available training resources for professionals who work in areas relevant to the process control and automation industries.
- **Standards and Guidelines** – This guide is designed to facilitate research on existing standards in the area of control systems security.
- **Incident Response and Reporting** – This document describes the proper procedures for a chemical company to report a cyber incident to ICS-CERT and how this can positively impact the Chemical Sector.
- **ICS Procurement Language** – This document provides example language that companies can incorporate into ICS procurement specifications.

Additional references and tools available to sector partners and stakeholders are the Cyber Security Evaluation Tool (CSET); the ICS-CERT 2010 Year in Review and Incident Handling brochure; and a newly developed, scalable, cyber tabletop exercise that is available at no cost and includes scenarios for both business systems and ICS.

Milestones related to metrics and secure information sharing are the next steps in the Roadmap implementation process.

Reaching Out to the ICS Community

The working group identified owner and operator, vendor, and government conferences as important venues to deliver presentations and distribute awareness DVDs about the sector’s work in this area. Owners and operators can obtain the awareness package free of charge by emailing chemicalsector@dhs.gov. It is also available for download on the Homeland Security Information Network–Critical Sectors (HSIN-CS) Chemical Portal.



> Resources Available for DHS Critical Infrastructure Partners

Infrastructure Protection (IP) sponsors a free online NIPP training course at <http://training.fema.gov/EMIWeb/IS/crslist.asp>. IP also has a trade show booth available for sector use. Please contact NIPP@dhs.gov for information on IP participation and/or exhibition at an upcoming sector event or to schedule a trained speaker for your event.

> Implementation Success Stories

IP continues to seek NIPP and/or SSP implementation success stories from the sectors to be shared with other critical infrastructure partners. Please submit suggestions or brief write-ups to NIPP@dhs.gov.

> NIPP News

NIPP News is produced by the Office of Infrastructure Protection. NIPP partners are welcome to submit input. To submit information for inclusion in upcoming issues, please contact NIPP@dhs.gov. Recipients of this newsletter are encouraged to disseminate it further to their critical infrastructure partners.

> Learn more about the DHS critical infrastructure protection program at www.dhs.gov/criticalinfrastructure.