NIPP Newsletter

Homeland Security

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 41: MARCH 2009

Topics in this Issue

Upcoming NIPP CIKR Events

- **APRIL 1-3, 2009**
  Annual Defense Industrial Base Critical Infrastructure Protection Conference
  San Antonio, TX
- **APRIL 15 & 16, 2009**
  Safeguard Iowa Partnership Regional Critical Infrastructure Workshop
  Des Moines, IA
- **APRIL 20-22, 2009**
  U.S. Society on Dams Annual Meeting & Conference
  Nashville, TN

NIPP-Related Activities and Events

DHS Helps Coordinate Security and CIKR Protection for Super Bowl 2009

The Super Bowl is more than just a game it is a major security planning effort that requires focus, collaboration, and dedication to ensure that the game is played without incident. The DHS Office of Infrastructure Protection (IP) played a significant planning and prevention role in securing this year's game, proving that collaboration works. Examples of IP's commitment to this effort include the following people and programs.

Protective Security Advisors from the Protective Security Coordination Division helped to create the overall security plan by addressing vulnerabilities and providing tools to support local law enforcement. A key element was IP's focus on ensuring seamless coordination among all Federal partners. Protective Security Advisors also conducted security assessments of the stadium, media center, practice fields, team hotels, and other facilities – identifying and mitigating potential vulnerabilities.

The Infrastructure Information Collection Division helped by providing detailed infrastructure maps, in physical and electronic formats, for use by planning officials, first responders, and incident management personnel. These maps showed the city of Tampa's critical infrastructure and key resources (CIKR) in each of the 18 sectors. Each map was accompanied by a detailed list of vital information for first responders, including contact numbers, addresses, latitude/longitude location, and vital facts such as level of voltage at electrical facilities or the amount of chemicals contained at chemical facilities. These data allowed officials to plan potential evacuation routes and reduce vulnerabilities, and gave first responders information at their fingertips to help them respond effectively to any type of attack or incident.

Data were also provided electronically through the DHS Earth and Integrated Common Analytical Viewer (iCAV) platforms, which provided up-to-date geospatial information for situational and strategic awareness to enable local authorities and decision makers to instantly identify CIKR, or to add layers showing vital resources such as medical facilities or evacuation routes. This capability gives decision makers and first responders the information they need to better prepare for, prevent, respond to, and recover from natural and man-made disasters.

The Office for Bombing Prevention conducted training on surveillance detection, improvised explosive device (IED) awareness, and protective measures for hundreds of private sector personnel especially those responsible for soft targets such as hotels, restaurants, and the stadium.

Super Bowl 2009 scored big for IP and the Nation's football fans. Despite the football season coming to a close, IP remains prepared for and ready to tackle ongoing CIKR protection challenges for its customers and partners.

DHS Set to Launch iCAV Next Generation

The Infrastructure Information Collection Division will soon release a new version of the Integrated Common Analytical Viewer (iCAV), a secure, web-based application that enables Federal, State, and local homeland security partners to view, analyze, and share infrastructure information in map form. The application is used to create situational awareness and aid in incident planning, response, and recovery.

The newest version, iCAV Next Generation, is expected to be released in mid-to-late April and will replace the previous version of iCAV originally launched in 2004. Also known as iCAV NextGen, the new application contains numerous architectural improvements designed to benefit users by dramatically shortening response time and enabling usage in low-bandwidth environments, such as joint field offices and mobile command centers. These enhancements also make it easier and faster for users to zoom, move around in, or add additional layers to a map. With a cleaner and simpler display, iCAV NextGen makes the application and its features more intuitive and user-friendly. Whereas the previous version's display contained a multitude of buttons and toolbars, iCAV NextGen features a single streamlined toolbar and an easy-to-navigate data layer window to provide direct access to Homeland Security Infrastructure Protection (HSIP) data sets.

Though it is a new application, accessing iCAV NextGen should be seamless. Users will be redirected from the previous version and will be able to log in using their current Homeland Security Information Network (HSIN) credentials.

After the release of iCAV NextGen, the iCAV development team plans to meet with user groups to collect feedback for future updates, such as adding new data sets or layers, live feeds, and new data query functions.

For questions or information on iCAV NextGen, e-mail iCAV.info@dhs.gov, call (703) 235-4949, or visit www.dhs.gov/iCAV.

2009 Critical Infrastructure and Key Resources Learning Series

More than 450 public and private participants in a recent offering of the 2009 Critical Infrastructure and Key Resources (CIKR) Learning Series discovered how timely and accurate data can assist their infrastructure protection planning, preparedness, response, and recovery efforts. Presented by Rick Driggers, Director of the Infrastructure Information Collection Division, this seminar provided a detailed look at the tools and resources used for the collection, management, and visualization of infrastructure data available to Federal, State, and local partners.

The Department of Homeland Security (DHS) Office of Infrastructure Protection sponsors these one-hour web-based seminars on issues of interest to CIKR owners and operators and key government stakeholders. The Learning Series is designed specifically to provide practical ideas for implementation and the latest information on infrastructure protection tools, trends, issues, and best practices.

More than 2,000 people participated in the DHS 2008 CIKR Learning Series, which covered such topics as Improvised Explosive Devices; The Role of Regional Coalitions in Implementing the National Infrastructure Protection Plan; Critical Infrastructure Protection Mission and Vision; The Roadmap for Integrating Critical Infrastructure Response as a Key Element of the New National Response Framework; among others.

The information provided in these webinars is useful to a wide range of CIKR partners, including emergency management professionals; systems, security, facilities, operations, and financial or risk managers; and others engaged or interested in infrastructure protection and resiliency efforts. For more information on the 2009 CIKR Learning Series, please contact Jeff Grunner at Jeffrey.grunner@dhs.gov.

Upcoming Learning Series Webinars:

Engaged Partnership for Disaster Response – April 22, 2009

Infrastructure Risk Analysis and Information Sharing Capabilities – May 20, 2009

To register for the Learning Series webinars, visit: http://www.dhs.gov/xprevprot/programs/gc_1231165582452.shtm

DHS and DOT Hold Joint Briefings Focused on Field Operations

In the spirit of cooperation and collaboration, U.S. Department of Homeland Security (DHS) components met with representatives of the U.S. Department of Transportation (DOT) for informational briefings focused on the field staff and teams devoted to transportation safety and security. Participants presented ten (10) briefings addressing various areas of field operations ranging from historically safety-focused transportation organizations to the security-focused operations of DHS operatives. The following field operations were discussed, along with their missions and roles engaging with the private and public sectors to protect critical infrastructure:

- DHS Protective Security Advisors
- TSA Federal Security Directors
- TSA Surface Transportation Security Inspection Program
- TSA Visible Inter-modal Protection and Response (VIPR) Teams
- DOT Motor Carrier Safety Inspectors
- DOT Federal Railroad Administration Rail Inspectors
- DOT Federal Highway Administration Inspections
- DOT Hazardous Materials Inspectors
- DOT Pipeline and Hazardous Materials Safety Administration (PHMSA) inspectors and engineers
- DOT Regional Emergency Transportation Coordinators and their role in the Emergency Support Function (ESF-1) under the National Response Framework (NRF).

DOT also provided a tour of its Crisis Incident Management Center (CMC), with a description of their operations during all-hazards events and interactions between the various transportation modes.

The Homeland Security Act of 2002, the Aviation & Surface Transportation Act of 2001, and the Implementing Recommendations of the 9/11 Commission Act all impose requirements on the Transportation Systems Sector. As a result, it is important for DHS and DOT programs addressing these requirements to coordinate both their voluntary and regulatory activities, to the extent possible, to maximize efficiency and minimize redundant burdens on the public or private sector.

News from the Sectors

Defense Security Information Exchange (DSIE): An Information-Sharing Partnership for the Defense Industrial Base

In 2007, several members of the Network Security Information Exchange (NSIE) who were also defense contractors discussed the formation of a similar organization to be focused on the Defense Industrial Base (DIB). The NSIE was established in 1991 as a subcommittee of the Network Security Telecommunications Advisory Committee (NSTAC). The Industry NSIE works with its Government NSIE counterparts to share information on protection of critical infrastructure and key resources (CIKR) in the telecommunications industry. The Defense Security Information Exchange (DSIE) was formed using a similar trust model developed among over 20 of the leading DIB companies. In February 2008, the DSIE was formalized under the DIB Sector Coordinating Council (SCC) as the Cyber Sub-Council. The members leverage their trusted relationships to share intelligence on cyber-related attacks, enabling industry partners to quickly alert others of any ongoing incident and share mitigation strategies for the protection of Department of Defense (DoD) CIKR under their control.

Information-Sharing Rules

The information-sharing rules are simple and modeled after those used in the NSIE. All members and their companies have formally signed a Non-Disclosure Agreement (NDA) that allows the sharing of information on three levels:

- Non-attributional (all information);
- For DSIE eyes only, not to be shared outside the group; and
- Public Domain information.

(more)

All information is considered non-attributional outside of the DSIE. All information is by default non-attributional and cannot be shared outside the constraints of the DSIE without permission from the data owner.

DSIE Structure and Membership Responsibility

There are two subcommittees within the DSIE; one for tactical, real-time information sharing about cyber events and a higher-level strategic subcommittee. The strategic subcommittee represents the DIB SCC in developing their strategic goals and metrics related to cyber defense as dictated in the DIB Sector-Specific Plan (SSP). The overall mission of the DSIE is to protect the CIKR under the control of the DIB. Since the vast majority of assets within the sector are controlled by the DIB contractor community, it is imperative that these assets are protected. The DSIE follows a multidirectional, networked information-sharing process, as defined in the NIPP. Within the networked model, information is shared both vertically and horizontally across companies within the DIB. As a subcouncil of the DIB SCC, the DSIE attends joint meetings with the DIB Government Coordinating Council (GCC), where the SCC and GCC partner to provide strategic direction through development of the SSP. Members of the strategic subcommittee of the DSIE represent the DIB on several joint cyber committees, such as the Cross-Sector Cyber Security Working Group and the annual plenary session of the Critical Infrastructure Partnership Advisory Council (CIPAC).

The DSIE also holds bi-monthly meetings where all members share information related to their specific company's cyber concerns. This sharing is done at a non-attribution level. Such sharing helps all companies within the DSIE to strengthen their cybersecurity posture. All members are required to obtain a minimum of a secret level clearance to enable future classified briefings when needed. The future goal of the DSIE is to expand membership in the tactical information-sharing subcommittee to include all DIB members whose responsibility includes protection of DoD's cyber CIKR. The DSIE will continue working within the DIB SCC/GCC structure for future partnering opportunities with DoD, the Sector-Specific Agency.

Summary

The success of the DSIE is the result of establishing the trust model used by the NSIE for so many years. The trust was built within several closely held networks involving personal relationships between cyber forensic personnel at the various DIB companies. With this as a backbone, the DSIE rapidly gained acceptance as more information was shared without an incident or breach of confidentiality. In today's expanding and persistent threat environment, it is important to build on these successful sharing models to combat attackers. All information sharing is done voluntarily within the confines of the NDA. The success of the DSIE also rests on the use of established tools and techniques for the rapid and effective sharing of threats and attack vectors. It is not uncommon for information to be shared with the entire membership within minutes. The DSIE will continue to expand membership through the DIB SCC structure following the guidelines set forth in the NIPP. As the DIB GCC seeks to engage a similar organization, the DSIE will be able to begin sharing information through the CIPAC process with members of that organization. The DSIE is also working with the UK Aerospace Defense Manufacturing Exchange to facilitate future information sharing between the US and the UK defense industries. The DSIE has now expanded to include over 28 companies that share information daily. The success and the strength of the DSIE process are due to the dedication of the individual members and their extraordinary commitment to this effort. Through their continued support, they have made the DSIE, their organization, what it is today.

For more information on the DSIE, please contact Steve Lines at steven.r.lines@saic.com. For more information on the DIB SCC, please contact William Ennis at william.ennis@ennisstrategic.com.

Dams Sector Activities and Updates

Consequence-Based Top Screen Methodology

The Dams Sector Coordinating Council (SCC) and Dams Government Coordinating Council (GCC), under the auspices of the Critical Infrastructure Partnership Advisory Council, jointly developed a Consequence-Based Top Screen (CTS) methodology to assist in identifying and characterizing a subset of high-consequence facilities, the failure or disruption of which could potentially lead to the most severe impacts. The Dams Sector established a joint GCC/SCC Top Screen Workgroup to oversee the development and implementation of the CTS methodology.

The CTS is available to sector partners through a user-friendly, web-based tool that considers different consequence categories, including potential human impacts, economic impacts, and disruption of critical functions.

(more)

The Dams Sector-Specific Agency is working closely with owners, operators, and regulatory agencies to complete the CTS process in an effort to identify those assets with the highest significance across the sector. It is clear that without a strong collaborative effort, progress cannot be made toward improving the security and protection of the Nation's CIKR.

If you have any questions, please contact dams@dhs.gov.

Dams Sector Quarterly Meetings

The Dams Sector (including the Dams Sector Coordinating Council, Government Coordinating Council, and the Levee Subsector Coordinating Council) recently conducted its regular series of quarterly meetings on February 10-12, 2009 in Las Vegas, NV. Dams Sector quarterly meetings provide sector members the opportunity to discuss the status of various ongoing collaborative efforts and initiatives, including the Consequence-Based Top Screen methodology web-based tool, reference documents, and exercises.

Members of the Dams Sector GCC and SCC Visit the Arizona Power Plant

The February meetings included sessions for the different workgroups established under the Dams Sector Council structure (i.e., Security Education, Information Sharing, Research & Development, Programs & Metrics, Top Screen), as well as a special session for State representatives (State Dam Security Panel). Invited speakers included Mr. Jeff Morgan from the Nevada State Fusion Center, who provided information on Nevada's critical infrastructure protection program.

On February 13, members of the Dams Sector participated in a site visit to Hoover Dam. Representatives from the Bureau of Reclamation provided a private tour of the facility, which included a behind-the-scenes perspective of the dam. Highlights of the tour included a walk-through of the powerhouse and police operations center.

The next Dams Sector quarterly meetings are scheduled for May 13-15, 2009 in the Washington, D.C. metro area. If you have any questions, please contact dams@dhs.gov.

Tennessee Valley Authority Meetings and Site Visits

Members of the Dams Sector-Specific Agency (SSA) recently participated in a series of meetings and site visits with representatives from the Tennessee Valley Authority (TVA) and various other critical infrastructure stakeholders, focused on bringing together Federal, State, and local agencies involved in dam safety and security. These meetings provided the Dams SSA with enhanced knowledge and understanding of TVA's system of dams, as well as the opportunity to visit TVA's Chickamauga Lock and Dam and Raccoon Mountain Pumped-Storage Plant facilities located near Chattanooga, TN, along the Tennessee River.

The meeting also allowed the Dams SSA and TVA to discuss application of the Consequence-Based Top Screen (CTS) methodology web-based tool to TVA facilities. The CTS methodology can assist in prioritizing those high-consequence facilities that may have the highest potential impacts resulting from failure or disruption. The collaborative effort between the SSA and TVA will be part of the overall sector implementation of the CTS web-based tool to identify high-consequence assets within the Dams Sector.

For more information, please contact dams@dhs.gov.

The Nuclear Sector Partners with DOE on Response Security Training

The Nuclear Sector-Specific Agency is partnering with the Department of Energy/National Nuclear Security Administration (DOE/NNSA) on the Global Threat Reduction Initiative (GTRI) to reduce and protect vulnerable nuclear and radiological material located at civilian sites worldwide. GTRI's Domestic Threat Reduction program works to further increase the protection of radiological sources located at public and commercial facilities in the United States. GTRI-funded services are provided at no cost and include security training and assessments, and security upgrades.

One major requirement of an effective security system is a well-trained and equipped response force that can respond to an event in a timely manner. To assist with this requirement, GTRI offers Response Security Training specifically for on-site or local responders that support the protection of sites with radiological materials. The Response Security Training is conducted at the U.S. Department of Energy's Y-12 site in Oak Ridge, Tennessee, and enables participants to receive hands-on training in a realistic setting using actual protection equipment. The classroom and operationally based training assists on-site and local responders to:

- Protect themselves when performing duties at locations known to use/store radioactive materials, to include training on "radioactive materials of interest";
- Protect themselves and the public during events involving radioactive materials through understanding, operating, and using personal radiation detection equipment;
- Experience realistic and operationally based scenarios that build on classroom instruction and hands-on exercises; and
- Learn in a flexible format with training conducted at multiple venues and tailored to specific response organizations, to include unarmed, armed, and off-site response personnel.

Scenarios are developed by Y-12 with input from the response community and are approved by the Office of Global Threat Reduction. The training uses mock-ups of realistic environments with real threat materials and includes responses to anomalous conditions and events, such as alarm activations.

For more information, see the following Frequently Asked Questions:

Who is the target audience for this training?

Security Force personnel identified in conjunction with GTRI.

What is the benefit to my institution?

This training will enhance your Security Force's ability to respond to attempted radioactive material theft or sabotage scenarios. Security Force personnel will be trained in the skills needed to respond to site alarms and protect themselves and the public.

When is the training offered?

Training events are conducted several times a year, allowing for scheduling at your convenience.

Where is the training held?

At the Y-12 National Security Complex in Oak Ridge, TN. The Radiological Response Training program is run by experienced professionals with armed services experience and radiological expertise gained at one of NNSA's highly secure facilities.

What will we learn?

The Security Force will gain hands-on knowledge in radiological incident response, enhanced security monitoring, communications, tactical considerations, establishment of perimeters, and radiological dispersal devices. Equipment training will focus on the enhanced surveillance assets and detection equipment provided by GTRI. This training is tailored as needed so responders can execute their own tactics and procedures.

How much will this training cost?

This voluntary program is FREE. All expenses (travel, meals, etc.) other than the trainee's training time, will be paid by the GTRI Domestic Threat Reduction Program.

The DOE/NNSA/GTRI contact for this program is Mr. Sonny Smith, 202-586-9265, sonny.smith@nnsa.doe.gov.

Resources Available for NIPP Partners

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 CIKR 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 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 CIKR partners.