Homeland Security

NIPP NEWS

IN SUPPORT OF THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

ISSUE 58: FEBRUARY 2011

Critical Infrastructure Activities and Events

IP's Behind-the-Scenes Support for Super Bowl XLV

IP's Super Bowl XVL field team: Front row l to r: Harvey Perriott (North Texas; Super Bowl lead); Phil Constantin (New Orleans); Kerry Spaulding (South Houston). Back row l to r: Dave Hunter (Baton Rouge); Steve Nicholas (IPRD Gulf Coast); Brian Ebert (West Section Chief); Glenn Moore (Oklahoma); Derek Matthews (Acting Branch Chief); Ron McPherson (South Texas); Bill Gleason (Indiana); Charles "Buck" Hamilton (West Texas).

The 45th annual Super Bowl game played on February 6 and the week-long series of preceding celebrations and events went without incident. It is common knowledge that a host of authorities work behind the scenes to ensure the success of National Special Security Events such as the Super Bowl, to boost security and ensure preparedness. Less well known is that Super Bowl security involves the entire region impacted by the event, because of the need to protect and prepare venues such as hotels, transportation hubs, team practice sites, and the many charity events, concerts, and other events leading up to the game.

Also less well known is that the Office of Infrastructure Protection plays a key role leading up to and during the game. IP's support for Super Bowl XLV began in 2009 and culminated in a week-long effort involving a robust field operations team supporting a large area at the heart of the Dallas-Fort Worth Metroplex. IP deployed one Regional Director and eight Protective Security Advisors (PSAs) to assist the PSA of the North Texas District, Harvey Perriott. As lead PSA, Perriott was deployed to the Federal Joint Operations Center (JOC) to facilitate communications between the National Operations Center, Emergency Operations Centers, and the Event Operations Center prior to and during the event while providing situational awareness of critical infrastructure to the Federal Coordinator. Other PSAs supported the myriad protective security activities across the Metroplex.

"This Super Bowl was unique not only because it was the first held in that venue, but also because of geography," Perriott noted. "There are 750 square miles and five area commands covering Dallas, Fort Worth, Irving, Arlington, and DFW airport." For example, the Pittsburgh Steelers stayed and practiced in Fort Worth, but the Green Bay Packers stayed in Irving and practiced in Dallas. Concerts and charity events were held at a number of sites throughout the Metroplex area. Perriott began working the event in September 2009 and supervised the many assessments and other activities and the collection of shared information into tools and map books used by the five area commands to prepare and maintain readiness.

Pre-game Preparations

In the months leading up to the game, IP PSAs and vulnerability assessment teams performed 28 vulnerability assessments and security surveys to identify vulnerabilities at key event facilities to inform event security planning and operations, and provided protective measure options to enhance security at those locations. This included 16 Enhanced Critical Infrastructure Protection security surveys, which assess a facility's physical security, security management, security force, information sharing, protective measures, dependencies,

Topics in this Issue

and basic cybersecurity aspects. IP also conducted six Site Assistance Visits, including use of the Computer-Based Assessment Tool, which generates a comprehensive visual guide to assist DHS, facility owners and operators, local law enforcement, and emergency response personnel in preparing for and responding to incidents at critical infrastructure facilities. To help prepare local first responders for the event, IP's Office for Bombing Prevention conducted three risk mitigation courses that trained 68 State, local, and private sector partners on critical infrastructure protection tactics and techniques. The IP team also participated in four Super Bowl preparatory exercises, including a tabletop exercise (TTX) with local malls in September and October 2010 and the FEMA Region VI Consequence Management TTX in January. In coordination with the National Geospatial Intelligence Agency, IP also developed 100 geospatial products in support of the Super Bowl, including 36 tables and 64 maps. "On a scale of 1–10, I'd rate this effort a '10' for complexity," Perriott noted. "I'd also rate it a '10' for success." PSA Bill Gleason from Indiana picked up the baton from Perriott at the end of the event, as preparations begin for Super Bowl XLVI, which will be held in Indianapolis.

For more information about IP's protective security advisor and other programs, visit www.dhs.gov/criticalinfrastructure.

NIAC Releases Two Influential Reports on Resilience

The National Infrastructure Advisory Council (NIAC) recently released two reports that recognize resilience as a critical component of ensuring continuity of services and minimizing the impact of infrastructure disruptions. *A Framework for Establishing Critical Infrastructure Resilience Goals* and *Optimization of Resources for Mitigating Infrastructure Disruptions* deliver specific findings and recommendations for making businesses stronger, communities better prepared, and the Nation more secure.

What Is NIAC?

NIAC advises the President, through the Secretary of Homeland Security, on protecting elements of the Nation's critical infrastructure that support various sectors of the economy. The Council's comprehensive studies draw upon the expertise of subject matter experts—including CEOs, homeland security advisors, State and local partners, and corporate security managers—to report specific findings and recommendations. NIAC reports have focused on policies and strategies of risk management, information sharing, and protection and resilience programs.

Speaking to the NIAC Quarterly Business Meeting last July, IP Assistant Secretary Todd M. Keil noted, "The DHS mission—and IP's in particular—is a shared mission, and the results of NIAC's work have always reflected this core principle. This partnership in mission is the foundation for our collaborative approach with our stakeholders. In the spirit of this partnership, NIAC studies provide DHS with new insights that are helpful to our own internal strategic deliberations and capability development efforts."

A Framework for Setting Resilience Goals

The Framework report was undertaken to develop a process to support critical infrastructure sectors in establishing goals to improve their resilience. The study builds on the NIAC's 2009 Critical Infrastructure Resilience report that provided a common definition of infrastructure resilience, but recognized that each sector applies resilience strategies and practices in different ways. The Council found that the two sectors studied in detail—electricity and nuclear—are highly reliable and resilient due to companies mitigating risks as part of day-to-day operations. However, the emerging risk landscape and specific challenges to increasing resilience must be considered in order to minimize infrastructure risks and improve resilience. One key result of the report is a detailed framework for setting, testing, and improving resilience goals that can be applied across the critical infrastructure sectors.

Achieving Resilience Through Common Understanding and A Regional Approach

The Optimization report supports the strategic approach to resilience cited in the National Security Strategy by detailing findings and recommendations that advance the goal of national resilience that is built on effective cooperation between various levels of government, owners and operators of critical infrastructure, local communities, and private citizens. The Council found that there is an existing structure and base of knowledge about resilience on which to build, including private and public sector leadership, lessons learned and model approaches, and an evolving understanding of interdependencies, vulnerabilities, and mitigation options. The Council also recognized the broad contributions of companies as service providers, employers, and partners in mutual-aid agreements.

Two key observations underpin the study's findings and recommendations. First, the Council stresses the need for an enhanced common understanding of resilience and supporting activities across all levels of government and in the private sector. Second, the Council recommends the transfer of knowledge, tools, and processes from national resilience planning to regional and local jurisdictions.

To learn more about NIAC or to access published reports, please visit http://www.dhs.gov/niac.

IP and George Mason University Launch Joint Initiative on Critical Infrastructure Higher Education Programs

The Office of Infrastructure Protection (IP) has launched a new critical infrastructure higher education initiative in partnership with the George Mason University (GMU) Center for Infrastructure Protection and Homeland Security (CIP/HS).

"Protecting and ensuring the resilience of our Nation's critical infrastructure is a top priority for the Department of Homeland Security. It is an important and evolving mission area that is vital in our efforts to preserve our way of life," noted IP Assistant Secretary Todd Keil. "The critical infrastructure higher education initiative will help to establish the solid academic foundation needed to shape the homeland security workforce for the future."

"The new initiative will create a comprehensive, unified education and training system that produces and sustains the leaders and workforce required to ensure the protection and resilience of the Nation's critical infrastructure," said Mick Kicklighter, CIP/HS Director. The higher education initiative is funded by IP, which leads the coordinated national program to reduce risks to the Nation's critical infrastructure from all hazards and to strengthen national preparedness, response, and recovery in the event of an attack, natural disaster, or other emergency.

"Infrastructure protection professionals must be able to assess risks and vulnerabilities and develop mitigation strategies. They must also be skilled in exercising leadership in crisis situations, enabling them to respond to catastrophes, rapidly restore critical capabilities, and prioritize rebuilding, if required," Keil said. "Courses that address critical infrastructure must be part of a holistic approach to homeland security education."

Many of the disciplines engaged in infrastructure protection, such as security, law enforcement, and emergency management, currently focus on the development and evolution of their own education and training programs. "Consequently, most of the focus is targeted to the respective profession in which it occurs or is delivered within the context of a specific industry sector," Kicklighter said. "There needs to be an ongoing commitment to establish standard [critical infrastructure] educational and training programs and to encourage the adoption and incorporation of these programs within the [existing] education systems, and that is exactly what the GMU-DHS partnership initiative does."

The project includes an assessment of existing critical infrastructure degrees, courses, and teaching materials across higher education. A four-month assessment, completed in September 2010, summarized offerings in higher education, identified best practices, ascertained unmet needs, and offered recommendations for improving infrastructure protection education. Now CIP/HS is developing new higher education curricula focused on infrastructure protection that will serve as a prototype for graduate courses and certificate programs. These curricula could be taught at colleges and universities in a number of different schools, including schools of business, public policy, engineering, science, health, and government.

Potential future activities include the development of a graduate certificate program based on the higher education infrastructure protection curricula and modification of an executive master's degree to provide an infrastructure protection concentration.

"Throughout this process, external experts from academia, industry, and government will review, critique, and provide advice on the project from their various perspectives," Kicklighter said. The resulting courses will be nonproprietary, and the materials will be made available to any interested university or institution.

One of the initiative's key objectives is to develop professionals who are equipped with the education and skills to understand the Nation's critical infrastructure protection and resilience missions. The program fosters the importance of collaborative work among critical infrastructure owners and operators and the public sector. "The critical infrastructure mission demands a professional, highly educated workforce and cadre of leaders at all levels of government and in the private sector. We are looking forward to partnering with GMU in this very exciting higher education initiative," Keil said.

News from the Sectors

Efforts Underway to Develop International Levee Handbook

Dams Sector partners are actively collaborating with representatives from the U.S. and European Union (Germany, France, Ireland, the Netherlands, and the United Kingdom) to develop an International Levee Handbook. This handbook will provide levee owners and operators and emergency responders with comprehensive guidance and international best practices regarding the operation, assessment, maintenance, monitoring, design, and construction of levees.

To support development of the handbook, the Dams Sector-Specific Agency (SSA) was selected to serve as the lead for Chapter 6, "Emergency Preparedness and Management," which will address international best practices regarding inundation modeling, development and implementation of emergency action plans, and incident response activities, including response to natural hazards and manmade incidents. As part of this effort, the Dams SSA is actively coordinating with public and private sector partners across the United States, including members of the Levee Sub-Sector Coordinating Council (LSCC) and Levee Government Coordinating Council (LGCC), to gain full support and participation in the development of the handbook.

The Office of Infrastructure Protection is participating in the development of the handbook by serving as a member of the U.S. National Backing Group, whose main roles and responsibilities are focused on ensuring that the content of the handbook effectively aligns with U.S. best practices. Other members of the U.S. National Backing Group include the LSCC, LGCC, and the U.S. Army Corps of Engineers, among other public and private sector organizations.

To date, several international workshops have been conducted to support development of the handbook, including a chapter development workshop held November 8-10, 2010 in Amsterdam, Netherlands. The next international workshop is scheduled for May 3-6, 2011 in Dresden, Germany.

For additional information regarding development of the International Levee Handbook, please contact the Dams SSA at dams@dhs.gov.

USCG Cyber Command Addresses Cyber Issues in the Maritime Domain

The U.S. Coast Guard, as the Sector-Specific Agency for the maritime mode of the Transportation Systems Sector, formed a Cyber Command (CGCYBERCOM) in July 2009 to:

- Identify, protect against, and counter electromagnetic threats to the maritime interests of the United States;
- Provide cyber capabilities that foster excellence in the execution of Coast Guard operations;
- Support DHS cyber missions; and
- Serve as the Service Component Command to U.S. Cyber Command.

Planned mission areas include maritime critical infrastructure and key resources (CIKR) cyber threat analysis, information sharing and awareness/training, vulnerability assessments, incident response and recovery, and computer forensics and analysis.

While the Coast Guard has existing law enforcement authorities and is responsible for all aspects of securing the Marine Transportation System (MTS), including telecommunications and computer systems, the challenges posed to the cyber domain require a combined response effort. The Coast Guard is working to establish lines of communication between DHS; DoD; State, local, tribal, and territorial government agencies; and industry to protect the MTS and maritime CIKR by improving their collective cybersecurity posture. Due to the MTS becoming increasingly dependent on cyber systems, it is critical that maritime partners cooperate to fully identify, assess, and manage threats to communications, information, and control systems.

In one of the first major projects to begin this effort, CGCYBERCOM will team with the Volpe Center to study control system vulnerabilities in the maritime domain. In addition to this work, CGCYBERCOM has begun outreach and awareness coordination with Captains of the Port, Area Maritime Security Committees, Port Readiness Committees, Harbor Safety Committees, and industry partners to share information, address threats, develop exercises, and consider the creation of standards and best practices. CGCYBERCOM continues to expand its capabilities and looks forward to engaging with its partners in all of these efforts.

If you would like more information on CGCYBERCOM's efforts in maritime CIKR protection, please contact LT Will Towers at William.A.Towers@uscg.mil or Mr. Scott Dickerson at Scott.A.Dickerson@uscg.mil. For additional information about the USCG's role as a Sector-Specific Agency, please contact Ms. Eleanor Thompson at Eleanor.E.Thompson@uscg.mil.

Save the Date for the 2011 Defense Industrial Base Critical Infrastructure Protection Conference

As the Sector-Specific Agency for the Defense Industrial Base Sector, the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs is pleased to announce the fifth annual Defense Industrial Base Critical Infrastructure Protection (DIB CIP) Conference. The conference will be held April 12-13, 2011, at the Sheraton Society Hill in Philadelphia, PA.

This year's theme, "DIB CIP 2020: Setting the Vision and Strategy for the Next Decade" reflects the DIB's urgent need to assess potential threats to assets, systems, and networks vital to the security of the United States over the next decade.

Assistant Secretary for Infrastructure Protection Todd Keil will address the conference about IP's efforts to strengthen regional infrastructure protection and resilience, the Critical Infrastructure Risk Management Enhancement Initiative, IP's cyber infrastructure protection activities in the Energy Sector, and the collaborative effort underway to create better metrics for measuring program success.

Other panel discussions and presentations will address complex threats such as natural hazards, economic turmoil, and terrorist activities, and their potential to disrupt both DoD missions and the private sector. With the high potential for loss of life, property, and critical resources, DoD and its public and private partners must collaborate on risk management approaches and truly understand the risks—threats, vulnerabilities, and consequences—associated with DIB infrastructure. Discussions will focus on combating potential threats and defining successful mitigation strategies.

Featured Speakers:

Sean O'Keefe, CEO, EADS North America

Assistant Secretary Todd M. Keil, DHS Office of Infrastructure Protection

Deputy Assistant Secretary of Defense (Cyber Policy) Robert Butler

Deputy Assistant Secretary William Bryan, Infrastructure Security & Energy Restoration, DOE

Invited Speakers:

Principal Deputy Under Secretary of Defense (AT&L) Frank Kendall

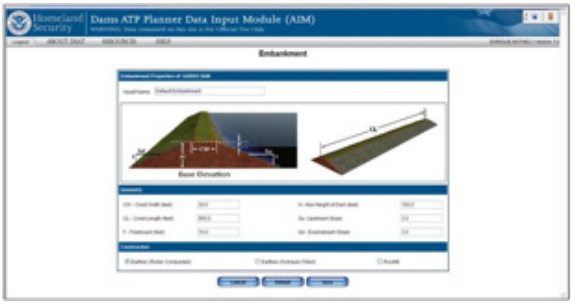
Rear Admiral Michael Brown, Director, Cybersecurity Coordination, DHS National Protection & Programs Directorate

This conference features key government and private sector experts and frontline practitioners involved in physical, cyber, and personnel security; information assurance; business and government continuity of operations; and preparedness. The wide range of topics and speakers demonstrates the complex issues surrounding DIB Sector resilience and highlights emerging and global threats.

For general information and to register for this unique, future-focused conference, go to: www.ndia.org/meetings/1030.

Dams Sector Develops Enhanced Capabilities in Blast Damage Assessment

The Dams Sector-Specific Agency (SSA) and the U.S. Army Corps of Engineers (USACE), through the USACE Office of Homeland Security's Critical Infrastructure Protection and Resilience Program, have collaborated to develop improved blast damage assessment capabilities to enhance the current understanding of potential damage levels resulting from a terrorist attack using explosive devices on dams. These joint efforts resulted in significant enhancements to the Anti-Terrorist Planner for Dams (ATPlanner-Dams), a software tool that provides approximate but realistic blast damage levels through simplified assessments based on generic attack vectors.



An initial pilot study conducted in the San Diego, CA area was completed in January 2011. The pilot provided a unique opportunity to apply the ATPlanner-Dams tool to several types of dams, including earth, gravity, and multi-arch structures, and culminated with the delivery of six reports to city and county officials. The reports contained the results of analyses of potential vulnerabilities and suggested protective measures that could potentially lead to a reduction of those vulnerabilities. In February, the Dams SSA and USACE initiated another collaborative effort with representatives from New Jersey to conduct a similar study involving several dams in the State.

Future collaborative efforts for blast damage assessments using ATPlanner-Dams will be facilitated through the Dams Sector Analysis Tool (DSAT), a Web-based tool providing Dams Sector partners with secure access to different modules and applications covering a wide range of analytical capabilities. For example, DSAT includes the Consequence-Based Top Screen (CTS) module, which facilitates

identification of high-consequence facilities whose failure or disruption could potentially be associated with the highest possible impacts across the sector. DSAT also supports the relative prioritization of dams based on a consequence index that reflects the overall potential for combined significant impacts. DSAT serves as the implementation platform for a conditional risk assessment methodology based on standard security configuration attributes and pre-selected attack modes and includes a database of dam incidents as well as supporting geospatial tools. Currently under development is an ATPlanner-Dams input module that will serve as a pre-processor for blast damage assessments. This module will consolidate the data required for scenario-based analyses, and the resulting input package can be submitted for subsequent ATPlanner-Dams analysis.

USACE and Dams SSA technical personnel will collaborate with dam owners interested in conducting blast damage assessment analyses. Priority will be given to high-consequence dams identified by the CTS process. For additional information regarding these blast damage assessment efforts, please contact the Dams SSA at dams@dhs.gov.

> 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.