Critical Infrastructure Partnership Advisory Council
Annual Plenary Executive Summary

October 13, 2010
Hyatt Regency Bethesda
7400 Wisconsin Avenue
Bethesda, Maryland
8:30am-12:50pm

Introduction

The Office of Infrastructure Protection hosted the 2010 Critical Infrastructure Partnership Advisory Council (CIPAC) Annual Plenary Conference on October 13, 2010. CIPAC was enacted to further the mission of the Department of Homeland Security (DHS) in the effort of protecting the Nation's critical infrastructure. The annual Plenary is a public meeting providing the public and industry members an annual update as to the activities, initiatives, and future goals of each the sectors and councils. The Plenary was co-chaired by the Assistant Secretary for Infrastructure Protection and Chair of the CIKR Cross Sector Council. In addition to representation from all 18 Sectors on the Council, the session attracted more than 100 attendees from the public and private sectors to engage in an open dialogue about critical infrastructure security and resilience planning.

The agenda focused on critical topics such as cross-sector interdependencies, information sharing opportunities, and challenges related to regionalization, and cybersecurity. The importance and need for effective partnerships at all levels of government and private sector to secure a safe and resilient nation was a common theme throughout the presentations and discussion. Speakers included Partners from the following Councils: CIKR Cross Sector Council, State, Local, Tribal, Territorial Government Coordinating Council (SLTTGCC), Regional Consortium Coordinating Council (RCCC), and the National Council of Information Sharing and Analysis Centers (ISACS)(NCI).

Two moderated panels stimulated lively and informative dialogue about sector accomplishments, initiatives, challenges and the path forward to strengthen the Nation's critical infrastructure. Panelists consisted of members representing DHS Councils, the Private Sector, Fusion Centers, the Information Sharing Environment, DHS Office of Cybersecurity and Communications, and DHS Office of Infrastructure Protection.

Deputy Secretary Jane Holl Lute delivered opening remarks and emphasized the Department's focus on ensuring a safe, secure and resilient place where the American way of life can thrive. She stressed the importance of enterprise and partnerships to secure the safety of the Nation. She discussed the five core missions outlined in the Quadrennial Homeland Security Review (QHSR) and highlighted the increasingly important mission of safeguarding and securing cyberspace.

The core missions are:

- Protecting against another terrorist attack;
- Securing our borders from dangerous goods and individuals while expediting legitimate trade and travel;
- Enforcing immigration laws to welcome those with good intent while preventing the entry of those with malicious intent;
- Ensuring a safe and secure cyber environment; and
- Creating a resilient nation of people able to withstand all risks and hazards.

Partner Remarks

Clyde Miller, Chair, CIKR Cross Sector Council
The CIKR Cross Sector Council is currently focusing on cross-sector interdependencies (particularly at the regional level), information sharing, and cybersecurity. An ongoing effort of the Council is to streamline the multiple requirements for information to reduce duplication of effort, which hinders the ability for a timely and comprehensive response. In addition, the Council made great strides in private sector participation in the planning and execution of National Level Exercises (NLE), particularly NLE 11.

Ulie Seal, Chair, State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC)
The SLTTGCC identified a series of goals for the upcoming year to include:

- Ongoing communication and collaboration with National Infrastructure Protection Plan (NIPP) partners;
- Further development of information sharing systems and planning networks with Sector Specific Agency (SSA) partners;
- Building regional partnerships;
- Continued discussion on Chemical Facility Anti-Terrorism Standards (CFATS);
- Enhancing the Automated Critical Asset Management Systems tool (ACAMS);
- Building an alliance network for the Council to identify and communicate with partners at all public sector levels; and
- Encouraging new and maintaining existing membership.

Tom Moran, Vice Chair, Regional Consortium Coordinating Council (RCCC)
Mr. Moran described the purpose of the RCCC as facilitating partnerships and coordinating regional efforts. To that end the RCCC outlined several goals moving forward:

- Completing the Regional Coordination and Resiliency Study;
- Creating a Common Attributes/Capability Catalogue;
- Organizing regional workshops to identify relevant regional areas of actionable potential and accomplishment;
- Increasing membership; and
- Continuing to educate each region as to its own threats and opportunities.

Will Pelgrin, Chair, National Council of ISACs (NCI)
Mr. Pelgrin informed the group that the name change from ISAC to NCI was to better represent the goal to ensure that every critical sector is represented. The NCI is building a directorate to determine how information can be shared both timely and easily through a digital dashboard or operations center. The ISACs have mapped their alert levels to a common alert level for better visibility, in addition to continued efforts in developing collaborative relationships with fusion centers. He discussed a pilot currently in progress for ISACs, representing multiple sectors, to share real time data and analyze that data from a cross-sector perspective. Mr. Pelgrin further commented that the NCI found participation in CyberStorm III very valuable and encouraged the involvement of other Sectors.

Roundtable I: Interdependencies and Regionalization

Panel Moderator:

- Ken Watson, CIKR Cross Sector Council, Senior Manager, Cisco Systems, Inc.

Panelists:

- Cherrie Black, Vice Chair, SLTTGCC, Bureau Chief of the Critical Infrastructure Protection Bureau for the New Jersey Office of Homeland Security and Protection.
- Jeff Dell, Northern California Regional Intelligence Center , Senior Vice President, Crises Management Strategic Planning and Industry Engagement Team, Bank of America
- Matt Morrison, RCCC Member, CEO, Pacific Northwest Economic Region (PNWER)
- Don Robinson, Regional Director, DHS Office of Infrastructure Protection

Mr. Ken Watson began the roundtable discussion by referring to interdependency as one of the Holy Grail issues of critical infrastructure protection. He noted that defining local and regional dependencies bolsters community resilience, ultimately raising the level of national resilience. The CIKR Cross Sector Council launched an interdependency initiative a year and a half ago with the purpose of understanding regional and local dependencies, beginning with a national level functional description of each of the sectors. Referencing past exercises and events, he noted that dependencies can be defined functionally at the national level, but information is really actionable at the regional and local level. The study began with a few sectors with the intent to validate the methodology through regional workshops to determine if this process can be used around the country to define local and regional dependencies.

Each of the panelists provided examples of how they approached regionalization and cross-sector interdependency efforts within their States or Regions. All reaffirmed the importance of the need for a trusted public-private partnership relationship to ensure that the work of building a resilient nation is successful.

The DHS Regional Resiliency Assessment Program (RRAP) cited five studies conducted in Chicago's Financial District, the Tennessee Valley, North Carolina's Research, New Jersey Exit 14 Turnpike Corridor, and New York State bridges. Ms. Cherrie Black further expanded on the New Jersey Turnpike Exit 14 RRAP, focusing on system recovery analysis examining interdependencies in five sectors along the corridor. Additionally, New Jersey is using the funding from the RRAP to develop a decision support tool to support prioritization of resources and efforts in a post-disaster scenario.

The Pacific Northwest Economic Region (PNWER) resilience programs emphasized the importance of conducting regional table tops, exercises and other assessment programs that facilitated information sharing among private-public partners. PNWER established the Center for Regional Disaster Resilience soon after 9/11 to specifically address critical infrastructure interdependencies, and designed a nationally recognized Blue Cascade series of interdependency exercises in the Pacific Northwest. Blue Cascades focused on both terrorist and natural catastrophic disasters and the resulting cascading impacts of critical infrastructure disruption in a five state international region.

Mr. Jeff Dell, Northern California Regional Intelligence Center (NCRIC), reiterated the importance of information sharing with the private sector by highlighting the success of the Infrastructure Protection Advisory Council, consisting of private sector partners across multiple sectors in the Northern California Region. Mr. Dell cited numerous accomplishments such as the Alert Notification System, weekly FOUO conference calls highlighting tips and leads as they are made available, classified and unclassified briefings, and access to the Homeland Security Information Network. The creation of the NCRIC Regional Portal, on the HSIN CS platform, allowed them to operationalize real time information sharing with their private sector partners.

Participants expressed concerns regarding availability of funding; the overall reluctance to share information, not knowing what is available with regards to national level or regional exercises, and the non-availability of after-action reports/lessons learned from the assessments conducted through the RRAP program. It was noted that funding will soon be an issue with regards to some of the exercises and other programs that require information sharing. The Department of Homeland Security (DHS) and the Federal Emergency Management Agency's (FEMA) grant programs have helped with funding in some areas, including two exercises that were sponsored by the DHS. The FEMA grant program provided funding to New Jersey, which helped to conduct three workshops dedicated to examining restoration, recovery, and governance in the wake of a long-term disruption to the Electric Sector.

Sharing of lessons learned/best practices was noted as a major challenge among the participants, including lack of knowledge about where to look for the information and the unwillingness on the part of the private sector to share the information. The reluctance of some in the private sector to share information on weaknesses or vulnerabilities mainly stems from how this information is protected once it is shared. The Protected Critical Infrastructure Information (PCII) Program was highlighted as a key to this process, but it is challenging to implement information sharing without a strong pre-existing

relationship with private sector partners. It was noted that there should be more education, training and outreach for the private sector partners on the benefits of sharing information, the various platforms within DHS to facilitate sharing, and the mechanisms in place to ensure that the information is protected. Deputy Assistant Secretary for Infrastructure Protection William F. Flynn commented that the growing element of success for information sharing is related to the trusted environment that we are working in, the protection that we can afford to the information, the feedback, the dashboards and the products that we can now provide to the private sector. It was recommended that one mechanism to improve information sharing would be for DHS to market the partnership model, specifically the Sector Coordinating and Government Coordinating Councils.

Participants raised concerns regarding lack of awareness at the local level of the national level exercises and activities, further illustrating the need for the RCCC and other initiatives such as the FEMA Lessons Learned website (llis.dhs.gov), which provides a valuable resource in the form of a calendar that identifies every exercise across the country.

Roundtable II: Information Sharing and Cybersecurity

Panel Moderator:

- Sue Reingold, former Deputy Program Manager, Information Sharing Environment

Panelists:

- RADM Mike Brown, Deputy Assistant Secretary, DHS Office of Cybersecurity and Communications
- Guy Copeland, Co-Chair, Cross Sector Cybersecurity Working Group (CSCSWG), Vice President, Computer Sciences Corporation
- Bill Flynn, Deputy Assistant Secretary, DHS Office of Infrastructure Protection
- Will Pelgrin, Chair, National Council of Information Sharing Analysis Center (ISACs), President and CEO, Center for Internet Security

Ms. Reingold introduced the topic of information sharing by referencing the President's Homeland Security Strategy which specifically calls for ensuring a secure and global digital information and communication infrastructure. From a national policy perspective this strategy recognizes the importance of strong leadership and partnerships to effect changes in policy, technology, education and perhaps law, to ensure a more secure and resilient digital infrastructure. Ms. Reingold commented on a July Government Accountability Office (GAO) report that highlighted the continuing challenge of consistently meeting public and private sector expectations regarding the exchange of useful, timely and actionable cyber threat information and alerts. To that end, she emphasized the importance of understanding all of the roles and responsibilities from a government and private sector, infrastructure perspective.

RADM Mike Brown opened the discussion recognizing the accomplishments over the past year and commented that we should continue to leverage and build off those successes. RADM Brown further noted that many CIPAC members were active

participants in the development, strategy, execution and now the after effect of the Cyber Storm III, the National Cyber Institute Response Plan, the National Cyber Security and Communications Integration Center.

The panelists discussed the complexity of integrating cybersecurity into the information sharing environment (ISE). There was an emphasis on information sharing as a shared responsibility between DHS and the private sector. RADM Brown commented that shared responsibility is part of the ongoing conversation about how we make sure we understand all the roles and responsibilities from the perspective of the government and the private sector. Some progress is being made on breaking the barriers and reluctance to sharing, with the focus now shifting towards determining what is important to share that is useful and actionable, and how to improve the efficiency of sharing information. The next layer of improving information sharing is examining capability and capacity, recognizing gaps and leveraging best practices.

Deputy Assistant Secretary William F. Flynn commented that this past year, IP encountered one of the most dynamic threat environments to date. He added that the Protective Security Advisor (PSA) program provides an important conduit of information flow between all levels of government and the private sector. Deputy Assistant Secretary Flynn discussed a new IP program that takes strategic/situational briefings to the regional level. These briefings have proven successful in five cities and he anticipates this program will continue to grow in the future. He further commented that the HSIN-CS architecture, from a macro, strategic perspective, provides the capability for information sharing with our partnerships. Future areas of focus are: cross sector information visibility and sharing, private sector participation in all hazards preparedness, and educational outreach.

The CSCSWG efforts were highlighted by noting that over 200 government and private sector members work within the partnership dedicated to securing our nation's cyber assets by contributing to ongoing policy discussions and development. This year, the CSCSWG contributed to the President's 60-day cyber security review and the examination of incentives in cyber metrics aimed at helping the sectors complete their bi-annual updates to their sector specific plans.

The Healthcare and Public Health Sector raised a comment regarding the emergence of the widespread acceptability of electronic medical records, indicating there are some operational benefits, but there is also an increased risk. The question was posed regarding any effort by DHS or the CSCSWG towards ensuring the security of the electronic medical records. RADM Brown indicated that indeed there is significant activity to examine the security of medical records related to potential regulations and standards. CS&C is working to articulate the threat, and to mitigate and reduce that threat through the use of standards.

What We've Learned and Path Forward

Assistant Secretary Todd Keil expressed his sincere belief that programs to mitigate risk to the Nation's critical infrastructure can be realized only when there is full and active participation of both government and industry partners. He noted that it is clear from the day's discussion that the success of public-private partnership is dependent upon effective collaboration and information sharing. He emphasized his commitment to listening to the ideas and concerns of the public and private sectors and that he seeks to incorporate that feedback into IP initiatives that are truly beneficial and meet the needs of our partners. Assistant Secretary Keil highlighted numerous initiatives for the path forward. He spoke of the continued expansion of the RRAP program as a model for implementing meaningful critical infrastructure security activities across the country. Additionally, he outlined efforts to regionalize IP and build critical infrastructure protection capabilities around FEMA's ten regions to enable the Department to better service its partners. He highlighted his commitment to expanding the role of the private sector in the development and execution of exercises, such as NLE 11, to further support our relationship with our regional State and local partners.

To enhance our ability to share intelligence, Assistant Secretary Keil outlined a new program entitled the Engagement Working Group (EWG). The EWG is a regional approach to sharing classified information with our partners in order to collectively develop mitigation measures for identified threats. He commented on a plan to further implement the NIPP that will more effectively track progress with the use of defined metrics. The Assistant Secretary also discussed IP's efforts to engage with foreign governments and international organizations in order to increase understanding of the interdependencies of critical infrastructure from a global perspective. In closing, Assistant Secretary Keil reiterated that the public and private partners that make up the councils are members of a unique partnership and that success is dependent upon effective collaboration and information sharing.

Closing Remarks

The Honorable Rand Beers, Under Secretary for the National Protection and Programs Directorate, Department of Homeland Security, emphasized that sharing meaningful and timely information with the public and private sectors is of particular importance to the Secretary of HLS. He further commented that the CIPAC Plenary is the highest level of aggregation of federal government, public and private partners and is an essential element of the overall approach by the Department and IP. Under Secretary Beers complimented IP's outreach efforts on the "See Something, Say Something" campaign, which further illustrates the Department's emphasis on sharing information and working together. He concluded the meeting by stressing that IP is listening and using what the partners say to make appropriate changes and accommodations to further strengthen the effectiveness of the public-private partnership.

Sector Representation

Banking and Finance GCC
Banking and Finance SCC
Chemical GCC
Chemical SCC
Commercial Facilities GCC
Commercial Facilities SCC
Communications GCC
Communications SCC
Critical Manufacturing GCC
Critical Manufacturing SCC
Dams GCC
Dams SCC
Levees SCC
Defense Industrial Base GCC
Defense Industrial Base SCC
Emergency Services GCC
Emergency Services SCC
Energy GCC
Oil and Natural Gas SCC
Food and Agriculture GCC
Food and Agriculture SCC
Government Facilities GCC
Information Technology GCC
Information Technology SCC
Healthcare and Public Health GCC
Healthcare and Public Health SCC
National Monuments and Icons GCC
Nuclear GCC
Nuclear SCC
Postal and Shipping GCC
Transportation GCC
Transportation – Aviation SCC
Transportation - Maritime GCC
Transportation – Maritime SCC
Transportation - Rail GCC
Transportation - Pipelines SCC
Water GCC
Water SCC