DEPARTMENT OF HOMELAND SECURITY

Critical Infrastructure Partnership Advisory Council 2012 Annual Plenary Executive Summary

October 3, 2012

Walter E. Washington Convention Center
801 Mount Vernon Place NW
Washington, D.C.

Homeland Security

Table of Contents

Introduction 2
Opening Remarks 2
Partner Remarks 2
Panel I: Physical and Cyber Critical Infrastructure Protection: Industrial Control Systems Security 3
Panel II: Building in Resilience: Addressing Aging U.S. Infrastructure 3
Panel III: Coordinated Effort in a Developing Situation 4
Presentation: Growing Partnership Opportunities at the Regional Level 4
Summary Remarks 5
CIPAC Plenary Agenda 6

Introduction

The Department of Homeland Security's National Protection and Programs Directorate (NPPD) hosted the 2012 Critical Infrastructure Partnership Advisory Council (CIPAC) Annual Plenary, which took place Wednesday, October 3, 2012. The meeting included discussions about cyber and physical security issues within industrial systems; addressing the need for repairs and replacements for aging infrastructure across the Nation; improving communications among all stakeholders during a developing situation; building more effective public-private partnerships at the State, local and regional levels; and activities being conducted within the critical infrastructure protection landscape.

Panelists taking part in the plenary identified opportunities to enhance the partnerships between the private sector and all levels of government to enhance the Nation's safety and resilience. The CIPAC Plenary furthers NPPD's mission to protect the Nation's critical infrastructure by offering a forum for public and industry leaders to provide updates on activities, initiatives, and goals within the 18 critical infrastructure sectors. In addition to representatives from the 18 sectors, a large number of partners, both public and private, engaged in open dialogue about critical infrastructure security and resilience planning.

Speakers and participants included representatives from the Sector Coordinating Councils (SCCs); Government Coordinating Councils (GCCs), Federal Senior Leadership Council (FSLC), Cybersecurity and Communications Division (CS&C), Partnership for Critical Infrastructure Security (PCIS); State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), Regional Consortium Coordinating Council (RCCC); and the National Council of Information Sharing and Analysis Centers (NCI).

Opening Remarks

Deputy Under Secretary Suzanne Spaulding, NPPD, and Charles Donnell, National Security Staff, emphasized the importance of the public-private partnership to accomplish the goals within critical infrastructure protection. It was noted that the critical infrastructure landscape has evolved into a network of physical, cyber, and aging infrastructure components, and without the vital expertise, capabilities, and resources of the partnership, it is impossible to protect our Nation's critical infrastructure.

Partner Remarks

Chairs from PCIS, SLTTGCC, RCCC, and NCI, as well as CS&C leadership, highlighted noteworthy developments, accomplishments, and areas that deserve focus, including:

- Reviewing all aspects of the current partnership to identify gaps and successes to improve information sharing and collaboration efforts, as well as assist with forming new and effective partnerships;
- Continuing to collaboratively work toward providing clear, concise, actionable, and accessible information about the complex risks that the Nation faces today;
- Reviewing the current and future priorities within each of the critical infrastructure councils to allow the alignment of similar initiatives, programs, and efforts;

- Using the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI) to cost-effectively prioritize our efforts and resources, and to measure progress against a set of risk management outcomes;
- Continuing to share information with State, regional, and local partners to gain better understanding of capabilities, needs, and processes; and
- Integrating cyber and aging infrastructure considerations into current and future critical infrastructure protection and resilience programs.

Panel I: Physical and Cyber Critical Infrastructure Protection: Industrial Control Systems Security

During the first segment, panelists representing the North American Electric Reliability Corporation (NERC), Dominion Power, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the National Institute of Standards and Technology (NIST) discussed the efforts to improve security for industrial systems, from both a cyber and a physical perspective.

Industrial control systems security was described as resembling a pyramid. Risk controls and surge risk controls — industry standards, and those security capabilities that an entity believes are within its ability to handle, respectively — make up the first two levels. But at the top level are those issues that are simply too big for any one site — for example, a small water utility or chemical processing plant — to process alone, and as a result require support from the public sector.

Participants also discussed the Information Sharing and Advisory Council (ISAC) system. Participants noted that while efforts have improved as a result of the ISACs, sometimes the only information shared is limited to what is mandated by standards or regulations, and is often insufficient to decisionmaking and response.

Panel II: Building in Resilience: Addressing Aging U.S. Infrastructure

The second panel featured representatives from DHS, the National Institute of Building Sciences (NIBS), the Federal Highway Administration (FHA), the American Society of Civil Engineers (ASCE), and the American Water Works Association (AWWA), who focused on aging and failing infrastructure in the United States.

Discussions centered on the investment necessary for repairs and upgrades, the benefits of pre-emptive maintenance, and the number of bridges, roads, and levees that are in near-immediate need of improvements. Among the aspects discussed was the D grade that the United States was given in the 2009 infrastructure report card produced by ASCE. The quadrennial report card estimated the cost of repairs and maintenance for the Nation's infrastructure at $2.2 trillion over the next 5 years. It was also noted that one-fourth of bridges are structurally deficient and require an annual investment of $17 billion for maintenance or replacement, an increase of $6.5 billion over current investment levels.

The concept of return on investment, and framing infrastructure funding as one of future savings rather than current expenditures, was suggested as a potential solution to the difficulties of convincing political leaders and business owners to fund such improvements.

Panel III: Coordinated Effort in a Developing Situation

This segment of the plenary focused on information sharing during a developing situation, and employed the expertise of representatives from the DHS Office of Infrastructure Protection (IP), PCIS, the Department of Treasury, the Water ISAC, and the Michigan Intelligence Operations Center.

It was noted that a particular challenge of information sharing is the coordination of the message, as there is no simple process for doing so across public and private partners. Posting information to portals — such as the DHS HSIN system — is useful, but not enough. This is particularly true in the context of cybersecurity threats, in which the speed of an attack does not allow for the typical time that information sharing takes.

The immediacy of threats during a rapidly developing situation requires a greater range of involvement from all levels of the critical infrastructure protection mission, in both the public and private sectors. The panel emphasized the vital need to identify the roles of government, Information Sharing and Analysis Centers (ISACs), and sector councils, to ensure clear and rapid transmission of information and avoid conflicts and confusion regarding responsibilities.

Presentation: Growing Partnership Opportunities at the Regional Level

The final segment examined the opportunities for developing partnerships at the regional and local levels, and drew on the experiences of the SLTTGCC and PCIS in establishing cooperative relationships.

Presenters explained that DHS/IP's Regional Initiative has been a key part of the effort to grow partnerships. The Regional Initiative has helped to establish a baseline understanding of critical infrastructure protection programs, both within State and local governments, as well as among critical infrastructure owners and operators. It was noted that the SLTTGCC examines and analyzes some of the critical infrastructure challenges that State and local governments face, but cannot propose solutions and best practices for all issues pertaining to governments. Some of the fact-finding and solution-building must be done at the ground level, and there is a need to get State and local governments working together to develop and sustain critical infrastructure protection efforts, especially when dealing with austere budgets.

DHS officials noted that the Regional Initiative demonstrates that the ability to convene public and private sectors to build partnerships is valuable, but improved communication among partners alone is not enough. The Department must also explore other options such as exercises or workshops, to bring stakeholders together to develop joint solutions for improving critical infrastructure resilience.

Summary Remarks

In closing comments, Caitlin Durkovich, Assistant Secretary of IP, and Robert Dix, Chair of PCIS, noted that the need to work together on all aspects of the critical infrastructure landscape is essential to ensuring a safe, secure, and resilient Nation.

Mr. Dix observed that successful infrastructure protection plans and exercises have been those that encouraged and actively courted the participation of the private sector, and that those efforts in which private sector critical infrastructure stakeholders felt disenfranchised or minimally engaged tended to produce unsatisfactory outcomes. Mr. Dix added that all CIPAC Plenary participants should recommit to the public-private partnerships in which they are involved, as the security of the Nation relies on nimble, effective, and efficient protection of our infrastructure.

Ms. Durkovich pointed to cybersecurity as one area in which public-private partnerships can be particularly effective and necessary, as the Nation's critical infrastructure is reliant on effective cyber protection. She also noted that there is a need for the Federal Government to use collaborative efforts as an opportunity to develop a better understanding of the private sector's needs, and to avoid complacency once a solid baseline of communication has been established. In addition, she acknowledged that infrastructure modernization is of particular interest to her, and that in the process of replacing aging infrastructure, issues such as resilience and security can be addressed at the roots and foundations of these new facilities and systems.

Visit www.dhs.gov/CIPAC for copies of the complete transcript and the 2012 CIPAC Annual publication.

Agenda

October 3, 2012

Walter E. Washington Convention Center, 801 Mount Vernon Place NW, Washington, D.C. 20001
ROOM 146 A - C

7:30 a.m. – 8:30 a.m. **Registration**

8:30 a.m. – 8:35 a.m. **Call Meeting to Order**

Caitlin Durkovich
Assistant Secretary, Infrastructure Protection (IP)
National Protection and Programs Directorate (NPPD)
Department of Homeland Security (DHS)

Robert Dix
Chair, Partnership for Critical Infrastructure Security (PCIS)

8:35 a.m. – 8:45 a.m. **Welcome**

Suzanne Spaulding
Deputy Under Secretary, NPPD, DHS

8:45 a.m. – 8:55 a.m. **Charles Donnell**
Senior Director for Resilience Policy, National Security Staff, The White House

8:55 a.m. – 9:00 a.m. **Roll Call**

Larry May
Designated Federal Officer, DHS

9:00 a.m. – 9:40 a.m. **Opening Remarks**

Federal Interagency Partners
Caitlin Durkovich, *Assistant Secretary*, IP
Chair, Federal Senior Leadership Council (FSLC)

Cybersecurity and Communications
Michael Locatis, *Assistant Secretary*, Cybersecurity and Communications, DHS

State, Local, Tribal, and Territorial Partners
Cherrie Black, *Chair*, State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

Critical Infrastructure Sector Partners
Robert Dix, *Chair*, PCIS

Regional Partners
Chris Terzich, *Chair*, Regional Consortium Coordinating Council (RCCC)

Information Sharing and Analysis Centers (ISACs)
Denise Anderson, *Chair*, National Council of ISACs

9:40 a.m. – 10:40 a.m. Physical and Cyber Critical Infrastructure Protection: Industrial Control Systems Security

Moderator: **Tim Roxey**, North American Electric Reliability Corporation

Panelists: **Mark Engels**, Dominion Power
Lisa Kaiser, Industrial Control Systems Cyber Emergency Response Team
Ronald Ross, National Institute of Standards and Technology
Marianne Swanson, National Institute of Standards and Technology

10:40 a.m. – 10:50 a.m. **Break**

10:50 a.m. – 11:50 p.m. **Building in Resilience: Addressing Aging U.S. Infrastructure**

Moderator: **Mike Kangior**, Office of Policy, DHS

Panelists: **Ryan Colker**, National Institute of Building Sciences
Emily Fishkin, American Society of Civil Engineers
Rebecca Lupes, Federal Highway Administration
Kevin M. Morley, American Water Works Association

11:50 a.m. – 1:00 p.m. **Lunch (On Your Own)**

1:00 p.m. – 2:15 p.m. **Coordinated Effort in a Developing Situation**

Moderator: **Tom Farmer**, *Vice-Chair*, PCIS

Presenters: **William F. Flynn**, *Deputy Assistant Secretary*, IP
Michael Arceneaux, Water ISAC
Leigh Williams, Department of Treasury
State Homeland Security Advisor/Emergency Manager **(PENDING)**

2:15 p.m. – 2:45 p.m. **Growing Partnership Opportunities at the Regional Level**

Presenters: **Cherrie Black**, *Chair*, SLTTGCC
Robert Kolasky, *Senior Advisor*, IP

2:45 p.m. – 3:00 p.m. **Break**

3:00 p.m. – 3:30 p.m. **Public Comment Period**

3:30 p.m. – 3:40 p.m. **Closing Remarks**

Rand Beers
Under Secretary, NPPD, DHS

3:40 p.m. – 4:00 p.m. **The Way Forward**

Robert Dix
Chair, PCIS

Caitlin Durkovich
Assistant Secretary, IP

4:00 p.m. **Adjournment**