Critical Infrastructure Partnership Advisory Council
2013 Annual Plenary
Executive Summary

November 5, 2013
Walter E. Washington Convention Center
801 Mount Vernon Place NW
Washington, D.C.
8:30 a.m. — 4:30 p.m. EST

Introduction

The Department of Homeland Security, Office of Infrastructure Protection (IP) and Partnership for Critical Infrastructure Security (PCIS) co- chaired the 2013 Critical Infrastructure Partnership Advisory Council (CIPAC) Annual Plenary on November 5, 2013. This Executive Summary provides a synopsis of the panel topics and participants' viewpoints from discussions on the implementation of Presidential Policy Directive-21 and Executive Order 13636, *Critical Infrastructure Cybersecurity*, situational awareness and information sharing in prevention and mitigation as well as response and recovery. A facilitated dialogue amongst the leadership of the sector and coordinating councils regarding critical infrastructure security and resilience priorities ended the day.

Panelists taking part in the plenary identified opportunities to enhance the national level public-private partnership structure at all levels of government. The CIPAC Plenary is an annual open to the public event to highlight activities, initiatives, and goals within the 16 critical infrastructure sectors and cross sector councils. The plenary convened leadership from the Department of Homeland Security's, National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP), the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), the Partnership for Critical Infrastructure Security (PCIS), the Regional Consortium Coordinating Council (RC3), the National Council of Information Sharing and Analysis Centers (NCI), as well as Government and Sector Coordinating Councils. Additional attendees included representatives from the 16 critical infrastructure sectors in addition to both public and private partners.

Opening Remarks

Opening remarks were provided by Department of Homeland Security Office of Infrastructure Protection Assistant Secretary, Caitlin Durkovich, National Security Staff Director of Critical Infrastructure Policy, Nitin Natarajan, and Partnership for Critical Infrastructure Security Chair, Robert Dix.

Ms. Durkovich commented on the panel discussions that were scheduled as well as the mission of the Office of Infrastructure Protection. She also emphasized that it is vital to determine how to raise awareness beyond the attendees of this meeting. Mr. Natarajan stated that critical infrastructure has transitioned to an all hazards approach. He also commented on the importance of understanding the role that cyber plays within this approach for critical infrastructure security and resilience. Mr. Dix stated that this meeting marked an excellent opportunity for government and private sector partners to move in a positive direction of improving critical infrastructure security and resilience and inform national priorities.

Partner Remarks

Chairs from the SLTTGCC, PCIS, RC3, and NCI each highlighted noteworthy developments, initiatives and accomplishments including:

- Critical infrastructure security and resilience efforts within the private sector as well as the state, local, tribal, and territorial community;
- Enhancing the public-private partnership structure through a diversity of membership within each Council and sector;
- Reviewing all aspects of the current partnership structure to identify interdependencies and areas where information can be shared to minimize threats;
- 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;

Panel 1: Critical Infrastructure Security and Resilience and Implementation of Presidential Policy Directive-21

The first panel included representatives from the SLTTGCC, the Information Technology Sector Coordinating Council, and the RC3 in addition to the Department of Homeland Security's Integrated Task Force. This panel discussed the implementation of Presidential Policy Directive-21 (PPD-21) and Executive Order 13636 (EO*) Improving Critical Infrastructure Cybersecurity*. The goal of these documents is to strengthen the partnership and integrate cyber and physical aspects of critical infrastructure security and resilience. To date, a great deal of work has been completed in the realm of information sharing, processes, and partnerships to improve upon the existing partnership structure. While significant efforts have been completed, the overall goal to strengthen the partnership is not yet complete. Recent findings from reviews will now need to be implemented to further strengthen and expand the partnership over the foreseeable future. This will include actions such as creating improved communication paths, increasing information sharing and situational awareness, and gaining a better understanding of partners.

A large part of the implementation of PPD-21 and the EO includes a rewrite of the National Infrastructure Protection Plan (NIPP) and the creation of a voluntary Cybersecurity Framework. These two documents are expected to guide how the public-private partnership functions, and how organizations can best protect themselves from cybersecurity threats, respectively. Panelists discussed concerns from some private sector partners regarding the current version of the draft NIPP and Cybersecurity Framework, stating that each document needs to be further reviewed to ensure they include all requisite topics and a path for effective and efficient adoption. For the NIPP, some concern was raised that a clear value proposition statement for industry and government to work together is not apparent in the draft. Other suggestions for inclusion to the draft were a more defined understanding of risk, investing in risk, and mitigating risk for the private sector. For the Cybersecurity Framework, it was noted that a sophisticated analysis of the cost effectiveness is missing. By not including this into the Framework, private sector entities may not be inclined to implement many parts due to the unknown cost of adoption. A full review and beta testing of the document and its implementation was recommended by a participant as a potential course of action.

Panelists agreed that progress still needs to be made in the public-private partnership; however, some of the panelists stated that the ability to stop and beta test an effort may not always be the most appropriate action. State and local entities need to begin implementation and cannot wait for the completion of beta testing. Predictive modeling and improving upon implemented activities are other ways to work to improve critical infrastructure security and resilience. It is understood that not every aspect of a plan can be predicted, and unexpected outcomes may arise. Having a trusted partnership where consistent ongoing collaborative discussions are conducted is a best practice to help mitigate and potentially eliminate unwanted consequences. Lessons learned from events such as Superstorm Sandy are opportunities to evaluate the capabilities of the partnership and determine appropriate next steps to improving communication, sharing of information and increasing situational awareness. Private sector input and the sharing of operational data has become valued information for critical infrastructure security and resilience. This type of information enables partners to more readily begin working towards becoming operational following an event, and therefore should be integrated into future planning.

Additional aspects to improve the partnership that panelists highlighted were the need to shift to an operations focus with an emphasis on collaborative efforts, increasing information sharing and timeliness of information exchange, maintaining a better understanding of partners and customers, and increased planning and activities at the grassroots level. Open communications were determined to be an important feature to improving the public-private partnership. Incorporating this piece into the partnership can greatly improve integrated planning, raise the knowledge base on cyber and physical threats, and maintain sustainable efforts.

Remarks from Acting Under Secretary Suzanne Spaulding

NPPD Acting Under Secretary Suzanne Spaulding stated that DHS is grateful for all the hard work contributed by all of the Councils within the partnership. She commented on the Presidential proclamation that November is Critical Infrastructure Security and Resilience (CISR) Month in addition to the importance of collaboration within the partnership. Specifically, NPPD has increasingly oriented the thinking, efforts, and work to ensure that the public-private partnership is supported. Leveraging insights and capabilities will help everyone make wise risk management decisions and assist response and recovery efforts when bad things happen. The vision of the utopia that is discussed with the NPPD staff is a world in which everyone has a perfect understanding of resources, capabilities and insights of each partner. There does need to be a sense of who can accomplish each task and goal. NPPD is listening to the feedback from partners and ensuring that feedback has impact.

Panel 2: Implementation of Cybersecurity Executive Order

The second panel included representatives from the Department of Homeland Security’s Integrated Task Force, the National Association of State Chief Information Officers, and the Communications Sector

Coordinating Council. This panel discussed the implementation of Executive Order 13636 (EO) *Improving Critical Infrastructure Cybersecurity*. Implementing EO 13636 continues with the three primary pillars: developing a Cybersecurity Framework, improving information sharing, and ensuring all efforts completed are inclusive with privacy and civil rights. To date, three incentives reports have been completed – one each by the Department of Treasury, Department of Commerce, and Department of Homeland Security, work has been conducted to improve dissemination of classified threat information internally and externally, and the Cybersecurity Framework continues to be developed.

The Cybersecurity Framework is currently in an open comment period. All partners are encouraged to review the draft document and make comments that may make the document more efficient and representative of their organizations. In addition, Executive Branch offices are reviewing the document to identify areas that may not fit with standards that are currently in place or contradict existing regulations.

Since the document is intended to be used in both the public and private sector, panelists raised concerns regarding the framework's adaptability to the variety of organizations due to their uniqueness of size, resources, and capabilities. The framework could become a hindrance if it is not applicable to all types of organizations due to their diversity within the partnership. While it is expected that the completed document should be able to be molded to the needs and capabilities of the user, it raises the question of the applicability of incentives if modifying baselines or best practices will keep organizations from obtaining them. These types of instances are continuing to be reviewed as a better understanding of the landscape and types of organizations is obtained. It was noted that on the Federal side, the Cybersecurity Framework does not currently have any binding aspects. The document is anticipated to be adopted by Agencies to show the benefits of determined best practices, with the expectation that other Agencies follow suit.

Identifying cyber dependent critical infrastructure efforts continue with the intent to identify organizations that maintain infrastructure which, if successfully incapacitated, would cause catastrophic consequences. It was emphasized that this effort is not intended to be a risk assessment on organizations, rather, it is being conducted to identify critical infrastructure. Outcomes are expected to give a better understanding of the infrastructure that exists, their functions, and dependence upon them. In addition, partners will understand what issues may become more prevalent in the future.

From the states' perspective, cybersecurity continues to be one of the primary threats reviewed and response efforts planned. State use of information technology has grown exponentially over the past few years, and this naturally creates potential targets. Cybersecurity specialists, such as Chief Information Officers, remain vigilant in protecting systems and databases from breaches and unauthorized usage. As states continue to move to more cyber oriented infrastructure, cybersecurity and associated best practices are required to be understood. Current barriers to ensuring more secure systems have been highlighted. There is an ongoing need to maintain an understanding from leadership and maintaining a high level of cybersecurity awareness for personnel. Training and processes continue to be developed in states; however, there remains a large task ahead to ensure personnel remains up to date on threats, training is continuing and effective, and plans incorporate all steps associated with critical infrastructure security and resilience including recovery.

Information sharing also remains important to partners as more systems become interconnected and codependent. Not only is information important, the language used, level of security, and sophistication of partners systems need to be considered to ensure the best and most efficient security measures are in place. It was emphasized that this task may be the most difficult due to the size, funding levels, and resources available partner differing.

The private sector also continues to work diligently with the public sector to ensure critical infrastructure is secure and resilient. In today's threat environment this includes cyber and physical programs. While collaborative processes are always evolving, the primary catalyst for good communications remains trust. Discussion within a forum of trust has enabled certain sectors, such as the Communications Sector, to collaboratively work to create Sector Specific Plans, reports, best practices, training, and conduits for information sharing such as the Communications Information Sharing and Analysis Center.

It is essential to build a trusted environment to discuss priorities. This is the only method by which true collaboration and information sharing can be accomplished. It is understood that agreement may not always be attainable, but the insights and knowledge gained from merely having discussions is just as valuable.

Panel 3: Information Sharing - Detection, Prevention, and Mitigation

The third panel included representatives from the Transportation Sector Rail Modal, the Transportation Security Administration, the Office of Infrastructure Protection, the Commercial Facilities Sector Coordinating Council, and the Wisconsin Department of Justice. This panel discussion focused on the use of information to create opportunities for critical infrastructure security and resilience through analysis and application of available threat information in the physical and cyber spheres.

Detection, prevention, and mitigation of threats to critical infrastructure are unique in many of the sectors; however, the key to ensuring the safety of the Nation can be greatly improved in all sectors by collaborative efforts within the public-private partnership. Through work being completed in the Commercial Faculties Sector and Transportation Rail Modal, models of successful partnerships have been developed. While each model is unique, general principles include maintaining specific focus for analysis, continuously collaborating and communicating with partners, sustaining efficient dissemination mechanisms, remaining vigilant in informing partners early, and obtaining feedback on completed work. By working to establish successful outcomes to each principle, detection, prevention, and mitigation of threats can be maximized.

Information sharing remains one of the primary components of infrastructure security, as well as one of the more difficult aspects of the partnership to effectively accomplish. It is a complex issue that needs to be examined thoroughly by partners in each sector. Who owns the information, who can it be shared with, what the classification of information is, do the networks have the capability to send certain information, what types of information do partners want, and the timeliness of information being shared all need to be understood in detail to create the best mechanisms to research, share, and disseminate information. In addition, maintaining a trusted environment to discuss sensitive information needs to exist for successful information sharing. Only when collaborative discussions are able to take place, can clear information that is both timely and relevant begin to flow on the nature of threats, types of information necessary to mitigate those threats, and products available to assist partners.

In addition to the ability to share information, the types of information requested is another issue that needs to be reviewed by partners. Difficulties have existed due to the nature of information requested from both the public and private sectors. Requesting broad, open-ended information causes undue stress on organizations and generally causes unnecessary work, incomplete data, or incorrect data. Focusing on specific requests greatly assists with obtaining informational needs and assists partners with a better understanding of the concentration on a sector.

From a state fusion center perspective, partnerships are the driving force in proper information sharing. There are 78 fusion centers across the nation with unique abilities, partners, and processes. This uniqueness represents a difficulty when attempting to partner with fusion centers. Building partnerships with as many centers as appropriate would be in the best interest of an organization. Connecting with fusion centers enables partners the ability to more readily share information and obtain a better understanding of local critical infrastructure security and resilience capabilities. In addition, by building upon partnerships, the private sector and the fusion centers are better able to determine how enterprises are connected and best practices used.

A wealth of information is already available to the critical infrastructure protection community that is either not utilized or underutilized. By incorporating the vast amount of information that is readily accessible, the base level of knowledge can be raised, partners can obtain a better understanding of best practices, and threats can be more readily understood and mitigated against.

Panel 4: Information Sharing - Response and Recovery

The fourth panel included representatives from the National Council of Information Sharing and Analysis Centers, the Real Estate and Communication Information Sharing and Analysis Centers (ISACs), the National Cybersecurity and Communications Integration Center (NCCIC), the National Infrastructure Coordinating Center (NICC), the National Operations Center (NOC), and the National Response Coordination Center (NRCC). This panel discussion focused on how operational centers come together during an incident to respond and recover as well as building steady state relationships.

Response and recovery is unique to every event and requires the ability to evolve depending upon developing circumstances. Some of the main components active during this phase of an event include the NCCIC, NICC, NOC, NRCC, and private entities such as the Sector Coordinating Councils and ISACs. Each of these entities maintains separate functions during and following an event but also coordinate with each other to maintain a level of awareness amongst all partners and develop a holistic picture of the event.

Much of the response and recovery phase of an event can be aided during steady state periods. It is during these timeframes that partnerships can be developed, communication pathways set up, and common operations can be created for usage during and post events. By sustaining common practices during steady state periods, the level of preparedness is greatly raised. Preparations and standard practices, however, are not the only factor to the most effective response and recovery. Projections, preparations, and common practices may not be appropriate during all events, as unintended consequences may develop. Accordingly, the ability to adapt and evolve quickly is necessary to maintain the best posture to respond. Some participants stated that there is also a need to turn various individual initiatives into a coordinated capability. Knowing your partners' capabilities, information needs, operational procedures, and goals is essential. It was noted that recent improvements to gain a better ability to disseminate and gather information from a local perspective include opening liaisons programs for NICC representatives to visit ISACs' security operations centers during events; creating local agreements with states for better access credentialing and communications; and bringing in additional partners like the fusion centers. These improvements assist with overall response and recovery efforts.

Cybersecurity efforts continue to evolve within the response and recovery phase. For the public sector, communicating a better understanding of how information is disseminated during an event is currently a factor that needs to be addressed to maintain a better security, recovery, and response posture, primarily within the private sector. As most of the cybersecurity threat information is voluntarily provided to the public sector, a trusted environment needs to be maintained for partners to submit information. This is true for private sector organizations as well. Without information, threats may go unnoticed and response tactics may not be instituted until drastic harm is inflicted. In addition to maintaining open lines of communication during an event, regular communications are necessary to create dissemination pathways for threat information.

Work continues to be conducted to improve gaps identified during events and exercises, with information sharing and communication being the primary focus. Having a holistic picture of an event and being able to get required information to all partners are two of the most important functions of response and recovery efforts. These two functions allow for the most complete understanding of what actions are necessary and the ability to direct and coordinate recovery efforts with limited interruptions. It was agreed that open and regular communication is the key factor to ensuring partners are collaboratively working to lessen identified gaps and build an operational partnership. With regard to communication, it was also noted that dissemination of information pertaining to analysis following an event is an area that can be improved upon. Information on post event analysis provides a simple method to raise the base level of knowledge following an event for all partners.

Panel 5: Critical Infrastructure Security and Resilience Priorities

The final session of the meeting was a facilitated discussion led by the Office of Infrastructure Protection, Sector Outreach and Programs Division amongst the Councils' leadership regarding the goals and priorities of each sector and the ultimate integration of those priorities into a set of National-level priorities. While each sector has a unique set of challenges and priorities for the future, an enterprise-wide review should be conducted to better understand the common goals and determine if collaborative methods would assist and mitigate duplications. In addition, obtaining a list of joint goals and priorities would allow for a better discussion with DHS leadership in determining on a path forward for the Federal Government.

From responses received prior to the meeting, Council leadership identified information sharing, preparedness and resiliency resources, and advancing cybersecurity as primary priorities. Information sharing was further divided into timeliness of threat information, improving cross-sector collaboration, and product development. Council leadership was then asked to further discuss the topic, concluding in identification of the following additional priorities.

1. Decrease the emphasis of the usage of pilots and increase the emphasis of broader operational implementation
2. Leverage the work that has currently been completed by the sectors, such as Sector Specific Plans to use as a starting point for cross-sector priorities and goals
3. Further interaction with the private sector to share information and improve the partnership
4. Integration of private sector into operations and evaluation of EO13636
5. Increased sharing of actionable information and improved coordination prior to, during, and after incidents and events
6. A request for increased discussion about moving into steady-state operations with PPD-21 and EO 13636
7. Increased examination of lessons learned within after- action reports from exercises such NLE; findings from regional reports and other partner interactions and using those as the basis for policy improvements and paths forward to address gaps in interdependencies
8. Increase the understanding of DHS goals and priorities to better inform both government and private sector goals and priorities
9. Increased communication about the partnership structure and rules of engagement.

Concerns were raised with regard to the timetable and method of this effort. To successfully determine the best priorities for the future, representatives suggested additional time to review the topic with broader sector memberships to obtain consensus, as well as break down broad topics into more directed goals that are sector specific. In addition, it was suggested that DHS present their goals and capabilities before each sector reviews their own priorities to allow for a more open and directed discussion with an understanding of the abilities and focus of the Federal Government.

Maintaining an updated set of goals for the overall critical infrastructure protection enterprise is essential to ensure partners understand each other's objectives and keep priorities progressing. It is understood that the environment is ever evolving, particularly with the ongoing implementation of PPD-21 and the EO, and the timing may not be opportune, but conducting these types of discussions at any meeting that have representatives from each sector will continue to raises partners' situational awareness on the differences and similarities between them.

Closing Remarks

The meeting concluded with closing remarks from Assistant Secretary Durkovich. She noted that the partnership is evolving as all of the partners continue to learn from one another. It is important to continue to move toward a safer environment and emphasize all efforts to limit the number of events that affect our critical infrastructure. An inclusive partnership recognizes that not all sectors share the same needs, but information sharing and collaborative efforts are important across all sectors. Critical Infrastructure Security and Resilience Month is a timely opportunity to examine resources and spread a message of security and resilience to protect our homeland.

Visit www.dhs.gov/CIPAC for copies of the 2013 CIPAC Annual publication.