Critical Infrastructure Partnership Advisory Council (CIPAC)
Plenary General Session
Executive Summary

Crystal Gateway Marriott
Arlington Ballroom, Salon III
1700 Jefferson Davis Highway, Arlington, Virginia

Tuesday, October 18, 2016
10:30 a.m. – 5:00 p.m. EDT

CIPAC Open

Renee Murphy, *CIPAC Designated Federal Officer (DFO), Office of Infrastructure Protection (IP), DHS*

The CIPAC DFO officially opened the CIPAC Plenary General Session. The official council member attendance and sign-in roster were validated.

Welcome

Caitlin Durkovich, *Assistant Secretary (A/S), IP, DHS*
Tom Farmer, *Chair, Critical Infrastructure Cross-Sector Council/Assistant Vice President, Association of American Railroads*

A/S Durkovich welcomed the attendees and thanked them for attending the first public CIPAC meeting since November 2013. During her tenure as A/S, public and private partners have worked under CIPAC to develop and mature capabilities in order to remain ahead of an ever evolving and complex threat environment. Since its formation, IP has worked closely with critical infrastructure owners and operators to support their risk management efforts. Highlights include:

- Enhancing information sharing capabilities between the Federal government and critical infrastructure stakeholders;
- Sponsoring security clearances for more than 2,000 individuals through the Private Sector Clearance Program;
- Working with fusion centers—as well as other Federal and non-Federal government partners—on a Secure Video Teleconference (SVTC) Pilot program to identify classified spaces around the country where cleared partners can receive classified information;
- Training more than 60,000 individuals through its Active Shooter workshops, as well as helping owners and operators develop their own active shooter plans;
- Working with vendors at the point of sale to raise awareness of explosive precursor chemicals through the Bomb Making Awareness Program (BMAP); and
- Sharing best practices and promulgating them across the 16 critical infrastructure sectors.

Recognizing that most of IP's customers are located outside of the National Capital Region, IP has recruited and hired 10 regional directors and begun the process of moving approximately 150 employees from its headquarters into the field. This will allow IP to more effectively coordinate with partners in the regions and provide them with the tools and resources that they need.

Mr. Farmer said that public-private partnerships like CIPAC exist and succeed because of the hard work and dedication of their participants. The underlying drive for this collaboration is the result of Sector-Specific Agencies (SSAs), sector representatives, Information Sharing and Analysis Center (ISAC) members, and other committed partners, working together to improve the partnership. He highlighted the main takeaways from the Critical Infrastructure Cross-Sector Council's meeting on October 17, 2016: identifying opportunities for improvement; collaborating with government to achieve goals; and building a strong partnership structure that can transition and continue to grow through changes in leadership.

Remarks

Suzanne Spaulding, *Under Secretary (U/S), National Protection and Programs Directorate, DHS*

U/S Spaulding acknowledged the strong leadership of IP and noted her appreciation for the public and private partners who had contributed to the enhancement of shared situational awareness in steady state and during incident response. Furthermore, the critical infrastructure security and resilience public-private partnership succeeds because of the participants' patience, perseverance, goodwill, and mutual respect.

She recognized DHS Secretary Jeh Johnson's ardent support of the public-private partnership model, serving as an important voice on their behalf in White House and interagency meetings. This support includes updating the National Terrorism Advisory System (NTAS) in order to make it easier to understand and use; supporting a unity of effort within the National Protection and Programs Directorate (NPPD) in order to take a holistic approach to cyber and physical security; and working directly with DHS employees to update the Department's mission statement: "With honor and integrity, we will safeguard the American people, our homeland, and our values."

Keynote

Jeh C. Johnson, *Secretary, DHS*

Secretary Johnson spoke about how the partnership structure described in the National Infrastructure Protection Plan (NIPP) continues to be valuable in addressing the protection of soft targets in the current threat environment.

Since his nomination in 2013, he has focused much of his effort on management reform within DHS, eliminating many of the stovepipes that hindered the Department's efficiency. This has been accomplished through centralizing hiring and budgeting processes; realigning headquarter functions; filling senior-level vacancies; and being more responsive to Congress. Highlights include:

- Proposing the restructuring of NPPD to become the Cyber and Infrastructure Protection Agency in order to align cybersecurity and infrastructure protection more closely;

- Establishing Joint Task Forces for border security in the Southwest and disaster recovery coordination in the Southeast; and
- The centralization and unity of effort across DHS, as reflected in the new mission statement.

Prior to these reforms, the Federal Employee Viewpoint Survey reflected low employee morale across DHS. The most recent survey response rates have improved and employee satisfaction was significantly higher, showing the largest single increase in any Federal department of DHS's size.

The Secretary also addressed how the global terrorist threat has evolved over the last 15 years from large-scale, directed attacks to smaller, terrorist-inspired attacks. DHS has had to adapt and become vigilant against homegrown violent extremism inspired by overseas terrorist organizations who recruit via the Internet. Combating these overseas threats with military force is only a part of the equation. At home, the FBI works to interdict terrorist plotting; the Department of State works with international partners to restrict terrorist travel; government installations have enhanced their security; and DHS partners with organizations like the National Football League and Major League Baseball to promote public awareness and vigilance.

In response to these threats, the Department has launched several initiatives. In December 2015, the NTAS was revised. Previously, alerts were issued only when there was a specific threat. The new system allows DHS to issue an intermediate level bulletin to describe signals or indicators the general public should be aware of, even without the presence of a specific threat.

Recognizing the critical role of community partnerships, DHS has facilitated outreach to Muslim communities to publicize the "If You See Something, Say Something™" (S4) campaign, helping them intervene in cases of potential self-radicalization.

In July 2015, the Transportation Security Administration (TSA) announced a 10 point plan for revising its aviation security programs. These reforms have resulted in reduced wait times at security checkpoints while still detecting and preventing foreign terrorist travel. This effort has been aided by customs officers conducting pre-clearance checks at the last point of departure from foreign airports for passengers traveling to the United States, and by conducting additional checks via the Electronic System for Travel Authorization. Finally, beginning in January 2018, driver's licenses issued by states not in compliance with Real ID Act standards will not be acceptable identification for air travel, adding another level of assurance of the traveler's identity.

Cybersecurity improvements are being implemented across the Federal government through the deployment of new technology—like the Einstein program—through the National Cybersecurity and Communications Integration Center (NCCIC). Einstein 3 – Accelerated (E3A) supplements the existing Einstein systems to block intrusion attempts, in addition to automatic, near-real-time sharing of cyber threat indicators across the *.gov* domain. So far, it has been deployed across approximately 75 percent of the Federal government and blocked more than 1 million intrusion attempts. It is expected to be fully deployed by the end of 2016 and will serve as a platform for future technology to block suspicious signatures.

On October 7, 2016, the Office of the Director of National Intelligence and DHS issued a joint statement formally accusing Russia of state-sponsored attempts to compromise the U.S. election process. DHS is now working with the states to help ensure the cybersecurity of their election systems.

Border security investments continue to make it more difficult for individuals to evade capture when attempting to enter the United States illegally. In the 2016 fiscal year, there were approximately 408,000 interdictions of illegal border crossings. This represents a significant reduction in number, but the demographics of those seeking to cross the border illegally are changing. There are now a greater proportion of families attempting to cross as they flee poverty and violence in Central America.

Lastly, FEMA has made great strides since Hurricane Katrina in 2005. It mobilizes quickly to deal with emergencies, supplementing state and local efforts to respond to and recover from natural disasters. Currently, it is working in the southeast to help communities rebound from Hurricane Matthew.

The Secretary closed by saying that he hoped to leave the homeland more secure, and DHS a better department, by the end of his appointment.

Council Remarks / Updates

Information Sharing and Analysis Centers (ISACs)

Denise Anderson, *Chair, National Council of ISACs/President, National Health ISAC*

The National Council of ISACs currently has 21 members and will soon be adding another. The ISACs strategic operations centers coordinate daily via cyber-focused calls. They also host weekly calls on physical threats and monthly Council meetings. Recently, the Council has started holding analyst meetings, following a recommendation from its exercise series.

The Council has contributed to national initiatives like the National Cyber Incident Response Plan (NCIRP) draft process and the Information Sharing and Analysis Organization (ISAO) standards development process. It leads the ISAO standards working group focused on guiding ISAOs to form and organize. It participates in biweekly classified intelligence forums to help inform the intelligence product development process. It has a member on the NCCIC floor to improve coordination and communication around incidents. Finally, the Council sponsored a 14 city public-private partnership Ransomware Roadshow to raise awareness, offer mitigation strategies, and emphasize the importance of information sharing.

Regional Partners

Chris Terzich, *Chair, Regional Consortium Coordinating Council (RC3)/Executive Board Member, InfraGard Minnesota*

The RC3's mission is to connect, enable, and foster public-private partnerships for the protection, security, and resilience of critical infrastructure within communities across the Nation. It is a "network of networks," ranging in size from single metropolitan areas to multi-state partnerships with some including international partners.

RC3 members participated in the NIPP Security and Resilience Challenge in 2016 to identify innovative ideas, technologies, and research to fill specific gaps in security, first responder needs, or other infrastructure capabilities. Four members' submissions were selected for funding:

- The Bay Area Center for Regional Disaster Resilience will produce and test a toolbox of products to enable cross-sector information sharing and decision-making.
- ChicagoFIRST will develop a Regional Coalition Web Portal and workspace for critical Financial Services Sector firms to use in conjunction with public sector agencies before, during, and after local emergencies that impact the regional and national economy.
- The All Hazards Consortium will advance the development of a sensitive information-sharing framework currently being incorporated by multiple states and private sector organizations within the Energy-Electricity Subsector as part of an ongoing East Coast effort used for regional disaster/disruption responses.
- The Cyber Resilience Institute will stimulate demand for cyber solutions by employing a community model, a marketplace environment, and tools and practical approaches that adopt commonly understood market force principles and characteristics.

The RC3 plans to continue its support of IP's regionalization efforts by identifying key private sector points of contact in each region. It will help connect other key regional organizations to expand the Council's capabilities, as well as those of newly-identified partners, to share information and best practices to increase regional resilience.

State, Local, Tribal, and Territorial Partners

Jory Maes, *Chair, State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)/Critical Infrastructure Program Director, State of Colorado*

The SLTTGCC is comprised of state, local, tribal, and territorial (SLTT) government officials tasked with providing their perspectives and expertise on Federal infrastructure protection activities and initiatives. The SLTTGCC also operates a Sector Liaison Program that establishes and maintains working relationships with the 16 critical infrastructure sectors.

The SLTTGCC's recent contributions to critical infrastructure security and resilience include:

- Commenting on the Advance Notice of Proposed Rulemaking on the Protected Critical Infrastructure Information program;
- Drafting the NCIRP;
- Sponsoring monthly "Real-Time Forum" webinars where Federal, SLTT, and private sector representatives convene to share information and discuss a variety of critical infrastructure topics;
- Publishing a Cyber Resource Compendium, which provides a list of programs and resources to small- and medium-sized SLTT programs looking to strengthen their cybersecurity postures;

- In conjunction with the RC3, publishing the Regional Overview of Critical Infrastructure Programs, which engaged more than 200 public and private sector critical infrastructure leaders to document the state of critical infrastructure mission implementation across the Nation; and
- Participating in the DHS SVTC Pilot that is leveraging fusion centers to share information securely and in real time with key sector contacts who can put that information to operational use.

Critical Infrastructure Sector Partners

Tom Farmer, *Chair, Critical Infrastructure Cross-Sector Council/Assistant Vice President, Association of American Railroads*

The Critical Infrastructure Cross-Sector Council supports information sharing in the current threat environment. The SVTC Pilot tested the sharing of classified information at secure locations around the country, allowing for more timely dissemination. Additional facilities and partners are being identified and clearances are being passed to fully implement the program. Work is still needed on sharing unclassified information through tear lines and providing guidance on what to share with partners.

The public has increased its reporting of suspicious activity in large part because of the S4 campaign. The public needs additional education on what types of activities should be reported, to whom they should be reported, and how reporting them makes a difference.

One of the Council's current priorities is streamlining the process for private sector personnel to re-enter restricted areas as part of incident response and recovery efforts. Much of the hard work can be done ahead of time by documenting the re-entry procedures for all 50 states before a crisis occurs. Government and industry should work together to examine the different solutions and leverage similarities to develop a more effective credentialing system.

Finally, with the upcoming change in Administration, both IP and the Council have committed to participate in joint government and private sector transition teams to set the partnership up for continued success.

Federal Interagency Partners

Caitlin Durkovich, *A/S, IP, DHS/Chair, Federal Senior Leadership Council*

In 2016, government and private sector members participated in more than 90 CIPAC meetings. This trusted environment facilitates the discussion of sensitive information and provides a forum for a variety of critical infrastructure security and resilience issues. The Calls to Action in 2013 NIPP, the development and release of the Joint National Priorities and the subsequent efforts made by the sectors to update their Sector-Specific Plans (SSPs), provide guidance for addressing these issues with a unity of effort. This is evident in the way the sectors developed implementation guidance for the National Institute of Standards and Technology (NIST) Cybersecurity Framework and in the implementation of cyber incident response protocols as directed by Presidential Policy Directive 41 (PPD-41). Recent sector activities included:

- The Chemical Sector holding its tenth annual Security Summit in August 2016;
- The Commercial Facilities Sector broadening its look at soft targets, promoting the rollout of the Hometown Security campaign to small- and medium-sized businesses;
- The Dams Sector developing a Cybersecurity Capability Maturity Model;
- The Communications Sector contributing to the National Security Telecommunications Advisory Committee (NSTAC) report on big data analytics;
- The Information Technology Sector coordinating with partners on implementation of the NIST Cybersecurity Framework and securing the Internet of Things (IoT);
- The Energy-Electricity Subsector developing research and development priorities;
- The Energy-Oil and Natural Gas Subsector continuing its coordination and information sharing activities; and
- The Water Sector broadening the scope of its chemical and bioterrorism risk assessments in collaboration with the Chemical Sector.

Panel Discussion Introduction

Bob Kolasky, *Deputy Assistant Secretary (DAS), IP, DHS*

The Joint National Priorities in the NIPP are a sound, enduring foundation that can be updated and built upon based on evolving risks and new Administration priorities. Current efforts to address the Joint National Priorities include:

- Widespread adoption of the NIST Cybersecurity Framework to combat cyber threats;
- Working toward the NCIRP under PPD-41;
- Addressing the impacts of long-term power outages; and
- IP's efforts to serve as a catalyst for increased regional collaboration and support for cross-sector efforts.

The panel discussions were designed to focus on government and private sector perspectives on activities and initiatives to address the Joint National Priorities; examine successes and opportunities; and offer thoughts on a path forward for addressing future critical infrastructure challenges.

Moderated Panel Discussions

Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure

Moderator: Bob Kolasky, *DAS, IP, DHS*
Panelists: Chris Krebs, *Director of Cybersecurity Policy, Microsoft*; Kathleen Judge, *Director, Risk & Compliance, National Grid*; and Thomas Kuczynski, *Chief Information Officer, DC Water and Sewer Authority.*

Panelists discussed the sector, corporate, and individual motivations for caring about critical infrastructure security and resilience and steps they have taken within their organizations. Trust is a primary factor in delivering services and products. Mr. Krebs provided the example of when security issues were revealed after Microsoft's release of Windows 98, Bill Gates stood down operations to focus on putting together a better product development model. Subsequent iterations of the operating system became increasingly trustworthy as investments in security were moved closer to the beginning of the development process. Ms. Judge noted accountability to customers, shareholders, and regulators also requires a thorough approach that includes ranking facilities' criticality and side-by-side physical and cybersecurity risk management. Mr. Kuczynski emphasized that delivering safe and reliable water service requires 24/7 technology operation, and the inherent difficulties are magnified by the variety of technologies and vendors the organization relies on to provide its services. This includes a number of information technologies that must be secured.

Cybersecurity is a significant part of a corporation's identity and branding, which was not the case 10 to 12 years ago. Resource allocation was discussed in terms of risk and at what point in the process resources are allocated. Ms. Judge said involving employees from across all areas of an organization provides a more comprehensive picture of the risk landscape. Calculating the potential losses associated with failure to secure an element of the operation drives home the importance of making a strong investment in cybersecurity. Fifteen years ago, it was difficult to get support from leadership, but now the importance of cybersecurity investment is more apt to be understood at the highest levels. Mr. Krebs said the spending emphasis had been shifting in recent years away from endpoint protection (e.g., firewalls). Organizations are now assuming that they have been breached and are focusing on mitigation strategies to minimize the impacts of an adversary gaining access to their systems. They are investing in segmentation, hunt teams, and other techniques to limit adversaries' mobility within the system and expedite the process of identifying them and stopping their access. Mr. Kuczynski said it is critical to be clear and open about the risks of failure to adequately secure systems. Organizations understand that a focused and committed attempt to compromise their systems could succeed. They focus on strengthening their respective abilities to sustain and recover from an attack to continue delivering service.

The benefits that organizations realize through their voluntary participation in CIPAC include information sharing and broadening awareness. Additional support to sectors and organizations through the NIPP partnership could include greater emphasis on security as an aspect of product design, providing unclassified tear line information for sharing actionable information, and recognizing interdependencies. Mr. Krebs suggested revisiting the concept of critical infrastructure in the United States, specifically with respect to the 16-sector approach. As technology advances, interdependencies increase to the point that the sectors can no longer be clearly separated from one another. As systems continue to converge, the partnership should take time to think about the implications on future operations. Mr. Krebs added that DHS has an opportunity to provide guidance on IoT security. Mr. Kuczynski said that there should be a greater emphasis on security as an aspect of product design so that users have a reasonable degree of confidence that there are no obvious deficiencies, rather than finding and having to address them once they become a problem. Mr. Krebs added that DHS has an opportunity to provide guidance on IoT security.

The recent NSTAC *Report to the President on Big Data Analytics* recommended further exploration of technological, behavioral, and organizational solutions for managing cybersecurity risk. Mr. Krebs felt it made sense to start with organizational risk and suggested establishing an equivalent of the Unified Coordination Group (UCG) to bring together government and core players in information and communications technology to address the issue. Ms. Judge and Mr. Kuczynski said human behavior was the greatest risk which encompasses insider threats, either through direct action or by providing access to an external bad actor intentionally or unintentionally. Investment in awareness training is key for any individual who uses an organization's network or internal systems. Ms. Judge noted that her organization had started an awareness campaign for employees that starts by asking, "What's the worst that could happen?" and showing the potential cascading effects of even small-scale security failures. She said employees tended to understand better the importance of good cybersecurity practices that way.

Build Capabilities and Coordination for Enhanced Incident Response and Recovery
Moderator: Michele Guido, *Business Assurance Principal, Southern Company*
Panelists: Kathryn Condello, *Director of National Security, CenturyLink/Vice Chair, Communication Sector Coordinating Council (SCC);* Brian Tishuk, *Director, Financial Services SCC*; and Neil Jenkins, *Director of Policy and Planning, National Cybersecurity and Communications Integration Center, DHS.*

The panelists first discussed the NCIRP developed under PPD-41 and how it enhances the work the partnership does in establishing recovery strategies for cyber incidents. The document was made available for public comment through October 31, 2016. Mr. Jenkins said the NCIRP is a response to calls from the private sector on how to organize response activities including asset response, threat response and support from the intelligence community. In the structure, the NCIRP establishes DHS as the firefighter, working to neutralize the threat and share information, and the FBI to investigate the circumstances of the incident. DHS acknowledges that the process is too complex to solve with just Federal government action, so private partners have been invited to participate in a working group to develop the plan. It leverages existing national doctrine (e.g., the National Incident Management System and the National Response Framework) to ensure that cyber response procedures are consistent with their physical counterparts, especially in instances when there are physical consequences to a cyber incident. Going forward, information sharing should improve not just during incidents, but also when indicators are identified that can be leveraged in future mitigation and response efforts. In addition, there would be a national effort to exercise the principles of the document included in the planning of any future exercises involving the Federal government.

Several examples of how the sectors are working with government to enhance its response capabilities were discussed. Ms. Condello said the Communications Sector's recent work has been the culmination of a long arc that began with outreach to partners in 2015 and sectors will have to drill down to establish specific procedures to operationalize the NCIRP. Mr. Tishuk said the Financial Services Sector has revamped its Sector playbook to connect with government, other sectors, and international partners to make it more robust and useful. It has also conducted exercises in conjunction with the U.S. Department of the Treasury. It has three other initiatives ongoing, which are focused on identifying gaps in public and private sector capabilities for responding to cyber incidents; mitigating the effects of attacks through backing up data for faster recovery; and enhancing information sharing and threat intelligence analysis. Mr. Tishuk described a recent joint cyber exercise conducted by the Financial Services Sector and the Electricity Subsector as a formal step in a cross-sector direction that had not previously been taken. It has been a valuable opportunity to build relationships and know who to contact during an incident. It is a precursor to institutionalizing solutions to gaps identified during the exercise.

Ms. Guido added that the Electricity Subsector had recently experienced successes associated with information sharing and threat analysis through partnership between public and private sector organizations. The NCIRP will help guide the Sector as it works to develop a cyber mutual assistance program.

The Sectors are seeing several advancements in information and threat analysis from their respective ISACs. For example, Ms. Condello said the Communications ISAC used various closed trust groups to facilitate the perpetual flow of information without over-sharing what might be irrelevant to some partners but is important to others. At the ISAC-wide level, information about suspicious network traffic can be shared and analyzed for legitimacy. At the next level, sector leaders engage in strategic conversations with the Federal government about issues of concern – for example, potential changes in vendor availability due to national and State politics.

In the wake of Superstorm Sandy and in anticipation of future events (including cyber incidents) that do not respect physical or political boundaries, the Electricity Subsector, Financial Services Sector, and Communications Sector are forming a Strategic Infrastructure Coordinating Council to address their sectors' interdependencies. Ms. Condello said it makes sense for these sectors to collaborate because they are heavily dependent on one another. They will start working from the sector leadership level to identify steps to engage effectively. Mr. Tishuk said that the Financial Services Sector relies so heavily on the other two that it is critical to institutionalize a structure that succeeds the individuals who create it. This is an opportunity to create a center of gravity for partnership between bodies that have the collective expertise to build a successful structure to address this type of issue. There will be opportunities to expand and replicate the model once it proves effective. The panelists agreed that many information sharing failures are due to reliance on individual relationships, rather than basis on an established process. A process-based methodology would be more viable.

Share Information to Improve Prevention, Protection, Mitigation, Response and Recovery Activities

Moderator: Shawn Graff, *Regional Director, Region VIII, IP, DHS*
Panelists: Bryan Paarmann, *Deputy Assistant Director, International Operations, Federal Bureau of Investigation*; Jory Maes, *Critical Infrastructure Program Director, State of Colorado/Chair, SLTTGCC*; and Fred Hintermister, *Manager, Cross Sector NERC Electric Information Sharing and Analysis Center (E-ISAC)/Vice Chair, National Council of ISACs*

The panelists provided examples of capabilities or programs built in their respective areas of responsibility and how they operate on "blue sky days." Ms. Maes said the State of Colorado had built a team of local law enforcement, Colorado National Guard, Colorado Bureau of Investigation, and FBI partners to address cyber capabilities. They quickly realized they needed more involvement from academia to anticipate what sort of cyber incidents the state might face. The team now exercises twice annually with critical infrastructure partners in the state. Through exercises and incident response, they realized that additional legislation and procedures needed to be enacted. Mr. Hintermister noted that there are different types of information sharing. ISACs are primarily focused on the "left of boom" information sharing that delivers resilience value.

The E-ISAC works to incorporate government and industry owner and operator knowledge to close gaps and talk about resilience opportunities, such as in the recent classified discussions on securing the grid. He encouraged executive- and operational-level individuals to build relationships before it is necessary to rely on them, because the process is more difficult during a crisis. Mr. Paarmann said the FBI's counterterrorism activities had shifted focus from investigation to mitigation. At the time of the September 11 attacks, the FBI had 23 Joint Terrorism Task Forces (JTTFs). That number has grown to more than 100. It has increased the FBI's ability to interact with local law enforcement to get information into their hands. It has also increased the number of interagency liaisons to break down walls between departments. The FBI is also working more with the private sector. It briefs private sector partners on threat credibility and provides intelligence based on their need to know. It can help them understand and link cyber and physical identities to counter homegrown violent extremist and insider threats.

There are several challenges to establishing information sharing processes with the private sector, and the panelists highlighted changes that are being made to address them. Ms. Maes said bringing partners to the table presents a challenge because of the lack of or minimal security clearance holders among private sector partners in the area, but she has observed a willingness to address this. There is not always a clear understanding of what private sector organizations can bring to the table, however the data they can contribute is a benefit and they are more willing and able to participate proactively in conversations and activities after being briefed. She also noted the importance of sharing information with State and local partners. It is important for local law enforcement and emergency responders to understand what elements of infrastructure are critical. Efforts are underway to make sure responders are aware of asset criticality so they can effectively tailor their patrol priorities and response procedures. Mr. Hintermister said organizations are doing a better job of configuring themselves to share information. As the dialogue continues, they discover more ways they can contribute. Finding the right information and knowing when and how to communicate it is how they can get to the tear line that is of interest to the private sector. For example, the 2013 Metcalf power station incident was an instance where good information sharing within the sector helped expedite the response and recovery, allowing power to be rerouted and mitigating the impact of the attack. Mr. Paarmann said the FBI was giving more sector-specific briefings; sharing classified information with senior leaders more frequently; and that after-action reviews were another important piece of the puzzle.

The panelists also addressed a question about responding to public inquiries regarding international incidents or events not directly related to their sectors. In many instances, sectors are relying on media for information; they do not know what is accurate and have difficulty responding to stakeholders. Mr. Paarmann suggested that sector partners could work through their local FBI field offices, or through attachés in U.S. embassies where incidents occur, for information. Mr. Hintermister noted that effective information sharing in these situations helps the sector avoid over-responding to incidents. Unity of effort and message are critical in such cases.

Future Opportunities and Challenges in Critical Infrastructure Security and Resilience

Moderator: David Kaufman, *Vice President and Director Safety and Security, CNA*
Panelists: Kirstjen Nielsen, *Founder and President, Sunesis Consulting/Chair, World Economic Forum Global Agenda Council on Risk and Resilience*; Pat Murphy, *Senior Director, Global Safety & Security Services Risk Management/Chair, Commercial Facilities SCC*; and Stephen Flynn, *Founding Director, Center for Resilience Studies, and Co-Director, George J. Kostas Research Institute for Homeland Security, Northeastern University*.

The panelists reflected on the discussions covered previously in the meeting and the challenges ahead. Ms. Nielsen said the environment had changed drastically in just the past few years due to factors like increased connectivity/digitization, resulting in increasing interdependencies, IoT, and aging infrastructure. There is a need to evolve and refine roles and responsibilities to secure assets, especially as cybersecurity becomes more important. An enterprise approach integrating physical and cyber risk is required. For example, IoT technology and supply chains need to be considered from end to end. Critical infrastructure also needs to be considered from a risk perspective, potentially leading to further differentiations within categorizations of critical infrastructure focused on systems, assets and networks at highest risk. Dr. Flynn said there needed to be a shift from a threat-centric to a resilience-centric mindset. Threat-centric thinking holds that intelligence-gathering entities should confirm whether there is a known-threat to an infrastructure sector as a precondition to making any significant expenditure of resources for safeguarding it. Alternatively, a resilience-centric approach understands that threat can be influenced by both reducing the vulnerability of critical infrastructure and the consequences from attacking it. This is because any given threat involves possessing both the intent and capability to cause harm. If adversaries face more obstacles to successfully carrying out an attack on infrastructure, they will need to muster more capabilities which imposes a limit on those who lack the means to do so. Further, if an attack yields no meaningful destruction and disruption, it undermines the intent to attack it in the first place. As a result, a resilience-centric approach where critical infrastructure is safeguarded regardless of specific intelligence that it is being targeted, ends up driving down risk by providing a deterrent for carrying out these kinds of attacks. Dr. Flynn agreed with Ms. Nielsen's observation that more effort must be made in developing a deeper understanding of interdependencies across infrastructure sectors if they are to be made more resilient. This translates into the need for closer public-private sector information sharing. Another imperative is that infrastructure be designed not just for efficiency and safety, but also to fail gracefully and recover and adapt from major disruptions quickly. Unfortunately, current business and financial practices too often generate disincentives for adopting more resilience designs. The challenge is to work across the public and private sectors to include the insurance and reinsurance industries to better align incentives to support resilience investments. Mr. Murphy echoed that there is not always enough emphasis on making a business case for investing in security and resilience. For instance, the new Homeland Security Active Shooter Workshop is an excellent opportunity for Chief Security Officers to share information and create a business case to take to their senior management that explains why investing in security and resilience saves money or may even generate revenue.

Secretary Johnson mentioned the increasing shift toward homegrown violent extremist threats, represents a shift for critical infrastructure owners and operators as well. Mr. Murphy said that the old style of terrorism involved a predictable method of planning, practicing, and executing an attack which offered many indicators and left open opportunities for interdiction. Now, people can radicalize themselves at home with little interaction or opportunity for detection. The indicators have changed and we are still working to discern them. Dr. Flynn said that many elected officials and the general public have been reluctant to acknowledge that government cannot be 100 percent effective in stopping these kind of attacks. However, it is important that the public sector in an attempt to express determination to prevent acts of terrorism, not end up overinflating expectations beyond what can be delivered. Particularly, in the face of homegrown terrorists, it is becoming increasingly important to respond nimbly once an incident has occurred in order to reduce the consequences. The recent New York/New Jersey bombing incidents are an example where an effective response resulted in the quick capture of the perpetrator. Further, the speed at which government can lower public anxiety by demonstrating that an event is not a widespread conspiracy is critical, especially as sectors become increasingly interconnected.

The United States' population is expected to grow beyond what the Nation's current infrastructure can support. Considerations should be made and steps taken to begin to address this issue. Ms. Nielsen said resilience and security are a public responsibility to which everyone needed to contribute. It requires partnership in which both the public and private sector play critical roles to avoid single points of failure, recognizing that no one entity has all the capabilities, capacities, and authorities to act. Consideration should be given to addressing vulnerabilities and potential incident consequences in building codes, insurance coverage, and cost sharing agreements. However, insurance and regulation cannot answer these questions alone. It will take progressive consideration of the components of infrastructure and how they can be designed to be resilient against specific threats and whether they can be prefabricated in controlled environments to have that resilience built in. Mr. Murphy agreed that building codes have difficulty keeping up with risk. Dr. Flynn noted that if crafted correctly, investments in resilience-building measures could be considered as something that advances competitiveness. Since there are no risk-free places to live or work and business operations are decreasingly tied to physical locations, companies will increasingly gravitate to those communities that are most resilient and abandon those that are not. A demonstrable ability to withstand threats and hazards and quickly recover when major disruptions do occur will be key to maintaining customer confidence. When the security value of deterring adversaries from attacking critical infrastructure is added to this, the result is a compelling case for stepped-up investments in resilience measures. Nonetheless, crafting the business case for addressing the interdependency issue remains a difficult one to make. This is because a given infrastructure sector is likely to make investment decisions based only on the direct costs it may incur if it is disrupted, and not the secondary costs to other infrastructure sectors who are dependent on them. Finding a way for the cost of investing in resilience measures to be shared among all those who will benefit from them is key. There needs to be an open, cross-sector discussion about this issue with which Ms. Nielsen agreed, highlighting the potential for systemic cyber risk. For example, every sector would be affected if Position, Navigation, and Timing (PNT) capabilities were interrupted. Each sector should understand its interdependencies and be aware of its responsibilities to other sectors that depend on it for their operations.

The panelists provided thoughts on the sector structure for critical infrastructure security and resilience moving forward. Dr. Flynn noted the asymmetry of capability and challenges across the various infrastructure sectors translate into it making more sense to tackle problems at the metropolitan or regional level then at the national level. This means getting planning, response, and recovery players on the same page and tied into regional capabilities. Sectors and regions have their own specific geographies, but they should be encouraged to share plans and strategies as partial solutions that can be modified and adapted by other regions. The Federal government can help them convene, engage, and sustain this important conversation. Ms. Nielsen said combining the regional and cross-sector approaches makes sense. It is important to have the right players at the table in planning activities, and government can help coordinate that. Mr. Murphy said the regional approach makes sense in the current landscape. It makes the message feel more personal and people are more likely to take it seriously.

The panelists also addressed a question from the Defense Industrial Base Sector on prioritization in a resilience-based approach of top-down coordination of national priorities by the Federal government. Ms. Nielsen said that Federal prioritization and guidance would focus on nationally-significant systems, networks, and interdependencies. Owners and operators would still have the responsibility to secure the assets over which they have control. This requires an understanding of the full risk picture from a national perspective. Dr. Flynn added that regional issues tend to be passed over at the national level. There is no such thing as truly national infrastructure; infrastructures can be divided into local, regional, continental, and global tiers (e.g., shipping; power distribution; communications). The national defense focus should make sure to incorporate both metropolitan/regional and continental perspectives.

Public Comment Period

No requests were received by the CIPAC DFO prior to the meeting. The public comment period was waived.

The Way Forward

Caitlin Durkovich, *A/S, IP, DHS*

A/S Durkovich said that meetings like this are beneficial to the broader owner/operator community. The summary of this meeting will be made available and posted to the CIPAC website. IP will also continue to work to bring additional critical infrastructure partners to engagements like this and will rely on the partnership participants to assist.

The CIPAC plenary included a wealth of information that will be important for the incoming Administration to be aware of. DAS Kolasky will remain in place during the transition to facilitate that process.

Information sharing is the backbone of the public-private partnership. Considerable strides have been made in automated indicator sharing and bidirectional information sharing, including sharing classified information when necessary and at lower classification levels when possible.

It remains important for the public and private sectors to engage and build relationships to more effectively address issues like the convergence of cyber and physical risk; include security in the infrastructure design process from the beginning; leverage technology to understand interdependencies and learn from previous incidents; and continue to make the value proposition argument that for every dollar invested in security and resilience, four dollars are saved on the recovery end.

To facilitate this, IP should shift its focus from asset protection to understanding interdependencies and the overall critical infrastructure landscape. There are many challenges ahead presented by new technologies and evolving threats, but by being a learning organization, IP is better positioned every day to mitigate against events.

A/S Durkovich thanked the meeting attendees for their collaboration and support during her tenure as IP's A/S.

Tom Farmer*, Chair, Critical Infrastructure Cross-Sector Council / Assistant Vice President, Association of American Railroads*

Mr. Farmer said that when margins for error are small, the fundamentals make a difference. The public-private partnership leaders in meetings like this are the ones who perform the fundamentals every day, ensuring that things are getting progressively better. The implementation of effective SSPs is just one measure of the progress made.

Partners are encouraged to take stock of what they have accomplished; get in touch with one another on projects of interest; and continue working together to bring creativity and innovation on infrastructure issues. He thanked the Federal government for its continued willingness to work with the private sector.

Adjournment / CIPAC Close

The CIPAC DFO delivered the CIPAC closing notice, adjourning the meeting.

Attendees were encouraged to complete stakeholder feedback forms and return them to the registration desk.