Critical Infrastructure Partnership Advisory Council

2018 Critical Infrastructure Summit

Summary

The 2018 Critical Infrastructure Summit—Critical Infrastructure Partnership Advisory Council (CIPAC) Plenary was held on March 1, 2018 at the Hilton Crystal City, Arlington, Virginia. Summit attendees included nearly 700 in-person and virtual public and private sector professionals, including CIPAC member organizations of the Government Coordinating Councils, Sector Coordinating Councils, and Cross-Sector Councils, and Federal Government agencies representing the 16 critical infrastructure sectors. The Designated Federal Officer certified the full-day Summit as CIPAC-compliant and validated a quorum of CIPAC member organizations was present.

This Summary highlights key themes from the 2018 Critical Infrastructure Summit. The opinions expressed by speakers at the Summit and captured below do not necessarily reflect the official position of the U.S. Department of Homeland Security (DHS).

Keynote

Secretary Kirstjen Nielsen, U.S. Department of Homeland Security

The mission to protect our critical infrastructure is too big and too complicated for any one entity to accomplish alone; partnerships are key, especially with the owners and operators who are integral to the resilience of the Nation's critical infrastructure that makes our way of life possible. A shared sense of purpose for building capacity and developing resilience guides the activities of CIPAC, the sector partnership, and its member representatives in addressing potentially systemic threats.

Security is a core business function of the United States' enterprises and a national competitive advantage. Maintaining that advantage requires a holistic, multisector approach that acknowledges the dependencies and interdependencies among the sectors. If we plan individually, we fail collectively.

Many threats and vulnerabilities to critical infrastructure exist. Among these threats, DHS has identified three major themes that were prominent over the past year and will remain significant for actions in the year ahead: soft targets, cybersecurity, and hurricanes.

Soft Targets—Preparedness is important and active shooter training can save lives. The first four responders to the San Bernardino, California, shooting in December 2015 were prepared to respond and readily work together despite never training together because of the active shooter training they had individually received. In the wake of the school shooting in Parkland, Florida, in February 2018, DHS is building on existing programs, providing education and awareness, and working with communities on preparedness-based engagement. The DHS National Protection and Programs Directorate (NPPD) is providing workshops and training to build capacity for detecting early warning signs as well as responding quickly to incidents. Hardening soft targets protects everyone. To that end, the DHS Science and Technology Directorate (S&T) has made innovative use of authority provided through the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) to work with organizers at large events and provide limited liability protections for deploying qualified anti-terrorism technology to enhance security.

DHS always seeks to better tailor products to users, so feedback is welcome. DHS is reviewing internal processes in order to streamline assistance to stakeholders. Closer collaboration between public and private entities is still needed to keep pace with dynamic threats.

Secretary Nielsen giving the keynote speech to open the 2018 Critical Infrastructure Summit. Photo credit: Brent Logan.

Cybersecurity—The Secretary identified three priorities related to cybersecurity: Address systemic or catastrophic risk through a collective defense model; protect government assets; and protect democracy into next election cycle. In the cyber domain especially, we are stronger as a group than individually. Attackers do not differentiate between public and private assets, and neither should those working to protect those assets. When the risk becomes systemic, private sector risk becomes DHS's risk and vice-versa. A cybersecurity strategy that builds on *Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* is forthcoming as well as a cyber supply chain risk management program that will help companies make better informed procurements decisions to mitigate risks. DHS has worked to create a unified approach to coordinating the people and tools needed to implement a layered defense of Federal computer networks, including the .gov domain. Development of dashboards that help DHS analysts identify and communicate about vulnerabilities across Federal networks has been central to these efforts. Finally, DHS is coordinating voluntary initiatives across the department and regionally, including an election task force led by NPPD to improve communications with state elections officials. In our democracy, it is vital to know that our votes are counted and counted correctly.

Hurricanes and Natural Disasters—In 2017, 25 million Americans were affected by storms. Hurricane Harvey was the costliest storm ever recorded with an estimated impact of nearly $200 billion. Preparation for future storms will save money in the long run. Sufficient funding now, such as through resilience grants, is essential to preparation efforts. Clarity on roles and responsibilities of stakeholders improves both preparation and recovery. The Federal Emergence Management Agency (FEMA) continues to work with state and local officials on both fronts.

Securing our shared critical infrastructure, which enables all aspects of our way of life, requires joint effort between government and industry. However, more work remains because security is not a destination, but rather a process of continual improvement that builds on a holistic, multi-sector approach to solving shared problems.

Welcoming Remarks

Christopher Krebs, *Senior Official Performing the Duties of the Under Secretary*, National Protection and Programs Directorate, DHS
Tom Farmer, *Chair*, Critical Infrastructure Cross-Sector Council

The Senior Official Performing the Duties of the Under Secretary, Christopher Krebs, welcomed participants to the Summit and explained that in pursuing its mission, NPPD benefits from clear communications. Therefore, NPPD is considering how to better align its name with its mission. Experience has shown that stakeholders who do not already know what NPPD does have trouble understanding what NPPD does. This situation was clear on the ground in Puerto Rico where local responders could readily identify FEMA, Transportation Security Administration (TSA), and U.S. Department of Energy (DOE) officials, but struggled to place the NPPD representatives. The name change to Cybersecurity and Infrastructure Security Agency as proposed in the *Cybersecurity and Infrastructure Security Agency Act of 2017* will clearly communicate the mission and offerings to current and future stakeholders and will help with morale and recruiting.

Critical Infrastructure Cross-Sector Council Chair, Tom Farmer, noted that CIPAC's strength draws from the real-world experience of hundreds of private sector representatives coming together to study their craft and share their skills. The next generation of practitioners will leverage these capabilities to respond to ongoing and emerging challenges. In particular, efforts today will equip people with the tools to respond to the threats they face. One example is the Secure Video Teleconferencing (SVTC) network, which supports rapid classified information sharing to wherever people are located when they need the information.

The sixteen critical infrastructure sectors are united by experience replete with commonalities. Meetings like this help identify the shared failures and successes and draw lessons learned that will help to improve future efforts.

Council Highlights

Jeremy Sroka, *Chair*, State, Local, Tribal, and Territorial Government Coordinating Council
Peter Ohtaki, *Executive Committee*, Regional Consortium Coordinating Council
Denise Anderson, *Chair*, National Council of Information Sharing and Analysis Centers
Tom Farmer, *Chair*, Critical Infrastructure Cross-Sector Council

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)—State, Local, Tribal, and Territorial governments are vital to protecting local assets and building regional capacity. SLTTGCC membership spans the ten regions, and is organized into six working groups examining a broad range of critical infrastructure issues such as unmanned aircraft systems, elections infrastructure, cybersecurity, information sharing, and national policy. The SLTTGCC is working with NPPD and FEMA to capture guidance and best practices for state and local officials to develop cybersecurity grant proposals and investment justifications that better align with the funding agency's expected policy outcomes. A communications strategy governs the SLTTGCC's outreach, which includes a new Regional Liaison Program to supplement the existing Sector Liaison Program to best represent the council and SLTT jurisdictions and reinforce person-to-person relationships to maintain trusted communications.

Regional Consortium Coordinating Council (RC3)—The RC3 comprises a network of networks, including more than 30 public-private partnerships operating at the local and metropolitan level, at the state level (e.g., California Resiliency Alliance), and at the regional and multistate level (e.g., All Hazards Consortium). Each partnership engages organizations and companies to work with government on collaborative planning for response to regional threats. Response to hurricanes and wildfires were prominent in 2017. RC3 members submitted projects for the National Infrastructure Protection Plan Security and Resilience Challenge, with several awarded funding for projects on unmanned aircraft systems (UAS), cybersecurity information sharing, and situational awareness information sharing that are showing tangible benefits in their regions. RC3 also jointly-hosts a series of webinars

with the SLTTGCC and DHS Critical Infrastructure Cyber Community Voluntary Program (C³VP) to educate stakeholders on a variety of cybersecurity issues.

National Council of Information Sharing and Analysis Centers (ISACs)—The National Council of ISACS (NCI) is composed of 21 ISACs whose missions vary from cyber focused to physical focused and cover all hazards. ISACs are celebrating 15 years of acting as trusted communities that share operational information with each other as well as best practices, incident information, indicators of compromise, and other useful information. Both the NCI and the individual ISACs continue to engage their communities on new threats and in exercises, which help uncover gaps to address. For example, the NCI held a forum on the cyber and physical threats at the Olympics, and they have shared information about the high-profile cybersecurity vulnerabilities, Specter and Meltdown. In 2017, the NCI officially welcomed its newest member: the National Defense ISAC.

Critical Infrastructure Cross-Sector Council—The Cross-Sector Council drew many lessons from hurricane preparedness successes and failures. The joint cross-sector development of a National Crisis Event Response, Recovery, and Access (CERRA) Framework informed access and reentry practices, allowing faster focus on the emergency at hand and better coordination among industry, county, state, and regional stakeholders. Experience in 2017 starkly demonstrated that life-enabling functions extend beyond food and water. For example, local water and wastewater treatment plant employees were essential to recovery, but as locals, their families' displacement by the storm hampers their ability to support the recovery. Beyond hurricane response, UAS have found both proper and improper uses, but misalignment between law enforcement's needs and Federal Aviation Administration regulations can and should be fixed. Finally, because adversaries take public reports of vulnerabilities and craft playbooks that exploit weaknesses to cause harm, the sectors may need to reconsider information protection guidelines.

Cybersecurity—The Way Forward

Jeanette Manfra, *Assistant Secretary*, Office of Cybersecurity and Communications, NPPD, DHS

Critical infrastructure owners and operators face many challenges to improving cybersecurity, and while DHS products help the community, the Department cannot solve all problems. Collaboration with industry and prioritization of actions are essential to moving forward.

Responding to cyber-attacks and breaches often depends on identifying and communicating with the right people to take advantage of their unique visibility into their own networks. Informal interpersonal relationships have been effective, but playbooks that help to quickly identify and connect the right people with authorities are needed.

Limited resources for enhancing security puts emphasis on addressing priority issues; both government and private enterprises will need to improve the cyber hygiene of their own networks. DHS has identified three priorities to support the critical infrastructure community in their efforts: human capital and workforce development, critical infrastructure risk management, and improved automated defenses.

Workforce Development—Many hundreds of thousands of cybersecurity positions remain unfilled in government and the private sector, in part because, as managers have reported, not enough qualified people exist in the industry. One projection estimates the shortage could grow to 1.8 million people by 2022. To mitigate the problem for the future, DHS promotes science, technology, engineering, and math (STEM) education, including computer science and security concepts, in K-12 curricula. DHS partners with the National Security Agency to certify higher education programs in cyber defense. DHS also participates in the CyberCorps® fellowship program, which funds scholarships to students in exchange for commitment to work in government for several years after attaining the degree.

Critical Infrastructure Risk Management—Critical infrastructure uses its assets to provide vital services and functions, so managing risk means examining not only the assets for potentially vulnerabilities, but also the essential nature of the functions to better develop resilience. Understanding the adversaries informs risk

management steps, so government intelligence resources should align to industry's information collection needs, where possible.

Automated Defenses—As automated information sharing from government to private industry improves, challenges still hinder automatically incorporating that information into cybersecurity defenses. Moreover, information sharing would be improved with greater collection from private industry back to government, who could anonymize data and distribute new insights. Every improvement raises the costs of cyber-attacks for adversaries and potentially prevents another owner or operator from becoming a victim.

Moderated Panel Discussion: Cybersecurity and Critical Infrastructure

Moderator: Tim Starks, *Cybersecurity Reporter*, Politico
Panelists: John Felker, *Director*, National Cybersecurity and Communications Integration Center, NPPD, DHS
John Davis, *Federal Chief Security Officer*, Palo Alto Networks
Stephen Dennis, *Director, Homeland Security Advanced Research Projects Agency*, Science and Technology Directorate, DHS
Kathryn Condello, *Director National Security / Emergency Preparedness*, Century Link

The moderated panel discussion on Cybersecurity and Critical Infrastructure afforded government and industry subject matter experts the opportunity to discuss the current cybersecurity landscape and answer questions from both the moderator and Summit participants.

The private sector has made great strides securing critical infrastructure against cyber-attacks. DHS has been working on these issues for 15 years. Most ISACs formed more than a decade ago and some originated before DHS's existence. CIPAC has been instrumental in fostering cooperation and collaboration between public and private stakeholders. Industry experts have called out many important issues where work is ongoing, including information sharing, elections security, industrial control systems (ICS) security, and threat deterrence.

Automation in Information Sharing—Increased automation enables quicker distribution of threat information, but humans still lead the decision making processes that rely on that information. Challenges with data access, aggregation, and analysis inhibit matching the right data and analytics with the right users at the right time. Operational details must be understood to instrument the data so that it is actionable. For the private sector to share data with the government to improve understanding of operational details, government must earn the trust of private sector by demonstrating strong data protection.

Private-to-Private Information Sharing—The Cyber Threat Alliance (CTA) is a successful model with an information-sharing platform based on essential indicators of compromise with range across the cyber threat kill chain. CTA requires member participation in the platform, both by providing their own information to share with all other members and by using the information shared by others.

Elections Security—DHS is working closely with state elections officials to address the existing, persistent threat. The designation of elections infrastructure as critical, on balance, is likely a positive step because it brings focus to the issue and more tools to bare. Security in this sector, however, is a tremendous challenge because elections are state-run enterprises with more than 50 different implementations. Securing these diverse technologies is hard, so DHS has conducted dozens of cyber hygiene studies with elections officials to begin to address the problem.

ICS Cybersecurity—ICS cybersecurity is extremely important. Many of these systems were built decades ago for specific locations and purposes with few, if any, requirements for network security. Catastrophic or systemic failure in these systems can cost lives. Modern information technology security acts as an effective first line of defense, but securing critical operational technology requires difficult upgrades that will take years as well as better understanding of adversaries. Control systems vendors have improved their products, and chief executives in sectors that have had incidents are fully engaged on the issue.

Threat Deterrence—Critical Infrastructure must make attacks more difficult and more expensive for adversaries. Economic and legal tools can be employed against nation state actors. International frameworks and rules for responding to cyber-attacks create entangled interests among nations and among private enterprises operating in those nations. Military deterrence should be the last option.

Divergence of Information and Security Technologies—Many trends in technology and security are headed in opposite directions. Technology has become simpler and more convenient to use, while security feels more complex and difficult. Fewer people are needed for the latest technology solutions thanks to greater automation, while security requires more people actively collecting information and aligning and investigating data. The internet of things brings greater connectivity throughout an enterprise, while security products tend to be built in isolation. Technology proactively solves problems, while security tends to react to incidents. Advances in technology may increase risk and introduce vulnerabilities, but the security industry must endeavor to address those issues while matching technology's convenience and usability.

Global Critical Infrastructure Trends 2035 and Beyond, A Paradox of Progress

Suzanne Fry, PhD, *Director*, Strategic Futures Group, National Intelligence Council, Office of the Director of National Intelligence

Recent and future global trends are converging and likely to influence critical infrastructure security and resilience in the next 20 years. The National Intelligence Council publishes a quadrennial Global Trends report to inform incoming or returning Presidential Administrations on global threats and trends relevant to national security and defense. Key themes from the 2017 *Global Trends: The Paradox of Progress* report relevant to critical infrastructure include the trends making governing more difficult, converging technologies, growing connectivity and economic uncertainty, and rising global tensions.

Global trends that are making governing and cooperation more difficult include the increasing number, complexity, and speed of threatening issues; increasing number of nation states exerting geopolitical influence; small groups exerting influence like nation states; and hardening of cultural or political differences and divergence through global information sharing. Government and the private sector are partnering to address these trends.

Converging technologies will accelerate world progress, but will also exaggerate interdependencies and discontinuities between industries and economies. Workers may be displaced and developing nations may see barriers to progress due to advances in automation and artificial intelligence. Healthcare and medicine will be revolutionized by biotechnology and may intensify moral differences between populations.

Growing connectivity of people and information across the world will increase the differences of ideas and identities and increase tensions and economic uncertainty between people and societies. Fractioned information and media tailored to specific groups will harden identities and be exacerbated by technological advances, such as identity algorithms. Tensions within and between nations will increase due to identity- and geo-politics. Terrorism will expand as the ability of malicious actors to conduct different kinds of attacks diversifies.

As the uncertainty of political and economic stability increases, businesses and governments that work toward resilience will see positive changes. The more resilient societies make investments in infrastructure, knowledge, and relationships to absorb and bounce back from adversity.

There is a concern that the rising confidence of adversarial world powers such as China, Russia, and North Korea could develop into significant threats if they overestimate their capabilities and act on their overconfidence. As populations expand, more dense civilizations increase the likelihood of major pathogens and diseases spreading. Between and among populations, the availability of healthcare creates a sharp dividing line of inequality. Though natural disasters will continue to be a major threat to critical infrastructure, achieving a high level of readiness is a solvable challenge. The partnerships and preparedness work between the public and private sector in the critical infrastructure space is a great example. Lastly, unforeseen issues that may arise from the combination of lower-

level threats should be studied to prevent strategic surprises. For example, corruption, environmental pressures, and socioeconomic pressures combined into a major series of events that comprised the 'Arab Spring' in Northern Africa and the Middle East.

Critical Infrastructure—The Way Forward

Bob Kolasky, *Deputy Under Secretary (A)*, National Protection and Programs Directorate, DHS

The successes of the partnership councils utilizing CIPAC reflect successes of government and industry working together at multiple levels to solve problems. However, room for improvement remains as this collaborative process continues to evolve in the face of threats that would attack our way of life. Through the CIPAC mechanism, work will expand to clarify and address problems around UAS, supply chains, insider threats, soft targets and the security of crowded places, nation state threats, social media's capacity to sow harm, and natural disasters.

Certain characteristics are common to the collaborative partnerships that best facilitate group problem solving. Reducing risk and removing vulnerabilities requires measurements to check progress and outcomes. Senior leadership engagement in both the public and private sector is needed to set appropriate priorities and budgets, which can keep momentum on these topics through leadership changes. Clear and frequent communication among stakeholders is essential to building trust. By building on a strong foundation of attributes like these will enable effective actions to solve problems.

Moderated Panel Discussion: Soft Targets – Crowded Places

Moderator: J.J. Green, *National Security Correspondent*, WTOP
Panelists: Bryan Paarmaan, *Special Agent in Charge*, New York, NY, Federal Bureau of Investigation
Doug Reynolds, *Vice President of Security Operations*, Mall of America / American Dream
Head of United Kingdom's Centre for the Protection of National Infrastructure

The moderated panel discussion on Soft Targets – Crowded Places afforded government and industry subject matter experts the opportunity to discuss current threats that we face today and answer questions from both the moderator and Summit participants.

Because of notoriety, soft targets and crowded places will continue to be attacked. The threat we face is the homegrown extremist and the active shooter, as well as the individual acting out the generic plans created to encourage that individual. Response must come from both the private and public sector by creating a culture of security, encouraging vigilance, and building in security early in new developments. Technology will be an assistive tool, when it can be deployed reliably.

Terrorist Publications and Copycat Attacks—Authorities in both the United States and the United Kingdom have faced many of the same low sophistication attack vectors, for example, vehicles as weapons and bombings outside an arena and inside a rail station. Part of the reason is that the threats and publications have created open-source playbooks for attacks, which anyone could potentially implement (e.g., renting then weaponizing a vehicle). Furthermore, terrorist publications and playbook authors often have direct communication access with a wide audience through social media and the internet.

Create a Culture of Security—Organizations and individuals should feel they play critical roles in security. Asking boards of directors, "Who is your security lead?" helps to create the culture where security is a top-of-mind issue. Individuals should know that speaking up when they see something will result in actions to reduce risks. Transparency and information sharing among police, private security, and shop owners creates a virtuous feeling of being on the same team, improving security.

Encourage Vigilance—However, the safer the public feels in public spaces, the less they feel the need to note minutiae. The challenge is to encourage people to stay vigilant and take action, but while fear can be a great motivator, in this context it more often exacerbates the vulnerability of crowds. One effective strategy currently in

use in some retail environments is greeting people and engaging them as they enter the property. Bad actors find the interaction unsettling, while average shoppers are reassured.

Build-in Security— One pathway to improving security is to consider it from the outset of construction of any new public space by implementing security by design. Asking urban planners to think about security from the beginning, obtaining buy-in from state and local first responders can improve security. Moreover, the building materials themselves can be improved: The UK has a program to encourage development and deployment of blast resistant building materials.

Combine Technology with Training and Standards—Technology can be a useful tool to applying security, but the capabilities need to match the threats. A technological solution might not fit well with the threat that needs to be mitigated. Often, barriers to use new technology fall into policy and process domains. For example, given a technological way to identify a large metal item in a crowd, the operator needs to know how the technology works and understands what authorities are in place to act on a positive identification. In turn, the operator needs to know what actions to take when there is a false positive. That said, technology is a tool and tools often require training, standards, and accreditation to use safely.

Moderated Panel Discussion: Hurricane Season 2017 Lessons Learned

Moderator: Rob Glenn, *Director*, Private Sector Division, Office of External Affairs, Federal Emergency Management Agency

Panelists: Dan Kaniewski, *Deputy Administrator (A)*, Federal Emergency Management Agency
Bruce Walker, *Assistant Secretary*, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy
Paul Stockton, *Managing Director*, Sonecon LLC

The moderated panel discussion on Hurricane Season 2017 and Lessons Learned afforded government and industry subject matter experts the opportunity to answer questions from both the moderator and several Summit participants as well as to discuss and build on each other's responses and experiences.

The hurricanes of the 2017 season offered many lessons, but none more so than Hurricane Maria, which illuminated challenges of responding to emergencies in relatively remote locations and the importance of preplanning and exercising to effective response. While Puerto Rico's electrical grid and distribution system was damaged, nearly 90% of infrastructure survived. Failures in planning and exercising to identify vulnerabilities at that local, state, and federal levels hindered the recovery efforts, as did delays in requests for mutual aid.

Importance of Mutual Aid Agreements—On the mainland, the framework for mutual aid among utilities works exceptionally well. In Puerto Rico, however, delays in requesting mutual aid were exacerbated by logistical difficulties in delivering that aid by sea or by air where ports, airports, and air traffic control were operating at reduced capacity. FEMA developed a triage plan to prioritize flights and make the impossible choices between immediate needs in the short term aftermath. Better planning before they are needed would have improved those plans.

Critical Infrastructure Interdependencies—The response to Hurricane Maria highlighted the importance of interdependencies among the critical infrastructure sectors. Restoring hospital services required water and wastewater services, which first needed power restored to those sites. Power restoration required coordination among communications, transportation, and financial sector infrastructure.

Resource Availability at the Local and State Level—Responding to Hurricane Maria, FEMA hit its own resourcing limits as a first responder working on the ground with the affected communities, a role it is not designed to play, in part because of diminished capacity at the local level where personnel needed to tend to their own families first. For example, whereas FEMA might usually rely on regional staging areas to distribute resources such

as food and water under standard operating procedures, in Puerto Rico, the National Guard had to step into that role.

Resource Availability at the Federal and National Level—FEMA not only faced challenges on the ground in Puerto Rico, but also found their readiness to deploy resources had been stretched thin. By the time that Hurricane Maria hit Puerto Rico, the response efforts to Hurricanes Harvey and Irma and to wildfires in California had severely depleted FEMA's resources, requiring reallocations. In the future, FEMA could rely on federally supported, state managed, locally executed plans, such as the efforts piloted in Texas to allow the state and local governments to use Federal dollars to manage and execute housing recovery.

Lessons Learned and Potential Next Steps—Several potential actions are under consideration that could improve response to future large and catastrophic disasters. FEMA could institutionalize best practices by creating a new emergency support function (ESF) explicitly focused on cross-sector planning, exercises, and mutual assistance. FEMA could conduct infrastructure sustainment and restoration operations that set a framework for triage when lives are at stake in large numbers. And FEMA needs a true accounting of the critical nodes and single points of failure when considering any and all hazards and vulnerabilities. Finally, FEMA's forthcoming strategic plan will seek to (1) foster a culture of preparedness, (2) enhance the capacity to respond to catastrophic disasters, and (3) reduce complexity of FEMA programs.

Public Comment Period / Closing of CIPAC

The following members of the public registered in advance to present oral comments to the CIPAC. Their spoken comments are transcribed in the separate Public Comment Appendix. Written comments submitted per the *Notice of Critical Infrastructure Partnership Advisory Council Critical Infrastructure Summit,* 83 Fed. Reg. 29 (February 12, 2018) can be found at www.regulations.gov by searching for docket number DHS-2018-0004.

- Dana Goward, Resilient Navigation and Timing Foundation
- Mary Lasky, InfraGard
- John Organek, Electric Infrastructure Security Council
- Charles Job, National Ground Water Association

The CIPAC Designated Federal Officer announced the closing of the CIPAC at the conclusion of the Public Comment Period.

Closing Remarks

Tom Farmer, *Chair*, Critical Infrastructure Cross-Sector Council
Dave Wulf, *Deputy Assistant Secretary (A)*, Office of Infrastructure Protection, NPPD, DHS

The 2018 Critical Infrastructure Summit speakers emphasized the importance of collaboration and leveraging the shared experience of stakeholders across the 16 critical infrastructure sectors, according to Tom Farmer. Summits like this one enable professionals to talk to colleagues directly and learn how things work in others sectors as well as from global thought leaders participating in the panel discussions. Lively discussion from participants and panelists alike pushes even the experts to think on their feet and ask "why not" in the face of complex challenges. Why not make the critical infrastructure that enables all aspects of American society more secure by continuing to push forward with this important work?

Deputy Assistant Secretary, Dave Wulf, noted that the various councils and working groups have developed and shared effective practices, define shared language, and clarified understanding of barriers to improving critical infrastructure protection. Everyone in attendance, in this community of security and protection professionals, has a significant role to take actions that move these practices beyond "demonstrated" and make them standard.