Critical Infrastructure Partnership Advisory Council

Year in Review

2017

Homeland Security

INTRODUCTION

Today's critical infrastructure risks extend beyond the ability of individual companies or even an entire sector to address—necessitating strong partnerships. During major incidents, owners and operators of today's critical infrastructure must work seamlessly across sectors and with all levels of government to rapidly respond and recover. Achieving this level of coordination in advance requires strong relationship building from the national to the local level. Public and private sector partnerships create the foundation for stakeholders to share information, characterize their risks, make informed investments, train staff, exercise response procedures, and ultimately build security and resilience into U.S. critical infrastructure.

Recognizing that private sector participation in the critical infrastructure mission is essential to strategic planning and effective information sharing, the Secretary of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) in 2006 as an advisory council exempt from the Federal Advisory Committee Act under which private sector partners may voluntarily collaborate with Federal Government agencies on critical infrastructure security and resilience efforts.

CIPAC enables the partnership structure approach defined in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* to promote, coordinate, communicate, and share effective practices across critical infrastructure sectors, jurisdictions, or specifically defined geographical areas. These objectives are achieved through a level of openness appropriate to support the homeland security mission, while maintaining a level of information surety needed for the private sector to be willing to share often-sensitive critical infrastructure information.

As depicted in the graphic below, CIPAC members are organizations representing government agencies, private sector owners and operators, and affiliated trade organizations and associations. For a complete list of CIPAC organizations by sector, please visit Critical Infrastructure Partnership Advisory Council Charters and Membership.

CIPAC Member Organizations

Federal Senior Leadership Council and Government Coordinating Councils	Critical Infrastructure Cross-Sector Council and Sector Coordinating Councils	State, Local, Tribal and Territorial Government Coordinating Council and Regional Consortium Coordinating Council
130+	700+	50+
Federal, State, and Local Government Departments/Agencies and Trade Associations	Private Sector Companies and Trade Associations	State, Local, Tribal, and Territorial Government and Regional Public Private Partnerships

PARTNERSHIP STRUCTURE

The national critical infrastructure partnership structures—including Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and cross-sector partnership councils—facilitate close cooperation and foster the trusted relationships necessary to manage critical infrastructure security and resilience in this inherently complex environment.

The councils regularly convene member representatives and subject matter experts from the private sector and government under the auspices of CIPAC to jointly plan and implement critical infrastructure programs; coordinate activities through joint strategies and roadmaps; and contribute to national policies, plans, and programs. As depicted in the graphic on the next page, the councils utilized CIPAC and the partnership structure to engage members and stakeholders in sector-specific and cross-sector events.

2017 CIPAC Meetings

142 Total

2	33	78	29
Joint Meetings of the Cross Sector Councils	Sector- Specific Full Council	Sector- Specific Working Groups	Multi-Sector Working Groups, Workshops, and Exercises

For additional information on the national partnership structure, please visit http://www.dhs.gov/criticalinfrastructure-sector-partnerships.

2017 ISSUES AND HIGHLIGHTS

Natural disasters, cyberattacks, and attacks on public gatherings challenged the security and resilience of the Nation's critical infrastructure during 2017. Partners across sectors responded through collaborative preparedness and response to emergencies, and ongoing developments in partnerships and information sharing. Key themes of these collective efforts for critical infrastructure security and resilience in 2017, as highlighted in this *CIPAC Year in Review*, include hurricane response, cybersecurity, security of soft targets and crowded places, the establishment of a new Election Infrastructure Subsector, the establishment of new cross-sector working groups, cross-sector collaboration and coordination, exercises and preparedness, and information sharing.

HURRICANE RESPONSE

The 2017 Atlantic Hurricane season was one of the most severe in recent history, with four Category 4 or 5 hurricanes that devastated communities in their path. Despite record-breaking losses and widespread deprivation from hurricanes Harvey, Irma, Maria, and Nate in U.S. Gulf Coast States, Atlantic Coast States, the U.S. Virgin Islands, and Puerto Rico, a coordinated approach across private sector industries and the Federal Government helped response and recovery efforts, largely through improved information sharing. The following are highlights of partners' efforts in 2017 in the wake of these natural disasters:

- From August to November, the U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) activated the Critical Infrastructure Crisis Action Team to support the response and recovery efforts for the landfalls of hurricanes Harvey, Irma, Maria, and Nate.
- Through joint NPPD and Federal Emergency Management Agency (FEMA) coordination calls with the private sector, interagency and cross-sector council partners were able to assess daily hurricane response needs and create essential coordination pathways to mitigate risks that could have substantial impact to critical infrastructure and the national economy. Throughout the 2017 hurricane season, over 40,000 stakeholders participated in these joint calls.
- NPPD and FEMA combined efforts to establish a National Business Emergency Operations Center (NBEOC) in Puerto Rico, which united with the National Infrastructure Coordinating Center (NICC) to facilitate access in hurricane-affected areas, enable businesses to resume, and support lifeline sectors' restoration.

- NPPD provided detailed hurricane analysis of likely consequences and cascading cross-sector impacts to critical infrastructure partners and stakeholders through advanced simulation and modeling tools. NPPD released nearly 100 new analytical products that were provided to over 23,000 subscribers across all levels of government and the private sector.
- The National Coordinating Center for Communications and the Communications Sector Information Sharing Analysis Center (ISAC) worked around the clock to support hurricane response and restoration efforts. These efforts included cellular service enhancement, activation of more than 465 telecommunications service priority requests, and completion of more than 5,000 calls through the Government Emergency Telecommunications Service and Wireless Priority Service Program for government and first responder partners.
- The Electricity Subsector Coordinating Council (ESCC) convened regular calls with industry chief executive officers and government officials, developed daily situation reports, and coordinated the industry's emergency power restoration mission following hurricanes Harvey, Irma, and Maria. Oil and Natural Gas SCC representatives held coordination calls with the U.S. Department of Energy (DOE), Energy Information Administration, FEMA, and other DHS components to ensure a common operating picture throughout response and recovery efforts.
- The FEMA NBEOC partnered with NPPD to establish a Business Infrastructure Industry Solutions Group. Its purpose is to facilitate unity of effort among Federal, State, and local authorities' crisis access and reentry processes to enable response and recovery operations, supply chain restoration, and resumption of business activities.
- The Financial Services Information Sharing and Analysis Center (ISAC) assisted during the aftermath of 2017 hurricanes by sharing credit card capability data with the NICC and the National Cybersecurity and Communications Integration Center (NCCIC) for distribution to resource vendors.
- The Healthcare and Public Health (HPH) Sector held daily coordination calls with the U.S. Department of Health and Human Services and private sector partners to identify challenges and potential cascading impacts of the hurricanes. Several HPH Sector manufacturers were critical resource providers for hurricane-affected areas and coordinated with Federal and State partners to mitigate shortages and medical emergencies for patients.
- The Emergency Services and Water and Wastewater Sectors leveraged the Emergency Management Assistance Compact process to coordinate an unprecedented multi-State, multi-utility deployment of emergency response crews to support utilities' response and recovery in the aftermath of hurricane Irma.
- An Incident Management Group was activated by the U.S. Food and Drug Administration to coordinate Food and Agriculture Sector response and recovery efforts for hurricanes Harvey, Irma, and Maria. Efforts included coordinating with FEMA on international support donations and coordinating with interagency and private sector partners regarding animal food and feed needs in impacted areas.

CYBERSECURITY

Critical infrastructure security and resilience extends beyond physical assets to the digital assets in information technology (IT) and industrial control systems. Threats range from sophisticated advanced persistent threat (APT) attacks to unintentional misuse of digital technology. In 2017, a number of cybersecurity incidents affected critical infrastructure owners and operators: the so-called "Dragonfly" APT; the ransomware WannaCry and NotPetya; and discovery and disclosure of malware targeting safety systems. Cybersecurity remains a top priority, made evident by the President's issuance of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, in May 2017. The following are highlights of partners' efforts in 2017 to improve cybersecurity across the critical infrastructure domain:

- The ESCC developed a series of operating strategies to guide grid operations following a major cyber and/or physical attack and expanded the Cyber Mutual Assistance Program to help companies respond to incidents.
- The Regional Consortium Coordinating Council (RC3)—in partnership with the DHS Critical Infrastructure Cyber Community Voluntary Program and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)—hosted a series of webinars with approximately 400 public and private sector participants on advancing cybersecurity and risk management awareness and best practices to address cybersecurity challenges facing critical infrastructure.
- The SLTTGCC published an issue paper on cybersecurity grant funding gaps and challenges for State and local jurisdictions. In partnership with NPPD and FEMA, the Council established a path forward to develop cybersecurity grant funding guidance and best practices for State and local jurisdictions.
- The Dams Sector developed the Dams Sector Cybersecurity Capability Maturity Model (Dams-C2M2) and the Dams-C2M2 Implementation Guide to advance the practice of cybersecurity risk management by providing organizations with a flexible tool to help them evaluate, prioritize, and improve capabilities.
- The Communications SCC produced a white paper to inform strategies for mitigating threats posted by botnets and automated cyber attacks. The paper defines the nature of botnet threats, the shared responsibilities of key stakeholders in the IT Sector for mitigating the threats, and opportunities for fostering greater collaboration among key stakeholders.
- The IT Sector established the IT Sector Resiliency Working Group to study industry and government approaches to cyber resilience and, as a result, developed the IT Sector "Cyber Resilience White Paper."
- The IT Sector updated and released the *Provide Domain Name Resolution Services and Provide Internet Routing, Access, and Connection Services Critical Functions Risk Assessment* in response to evolving policy and the technological internet environment. The assessment discusses current and potential risk management and mitigation activities for domain name service and internet routing, two critical functions that underpin nearly all infrastructure supporting global Internet communications.
- Defense Industrial Base Sector partners collaborated on implementing the security requirements of the National Institute of Standards and Technology Special Publication, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, in accordance with the Defense Federal Acquisition Regulation Supplement cybersecurity requirements.
- The HPH Sector released the *Healthcare Industry Cybersecurity Task Force Report* to identify gaps and challenges in advancing cybersecurity practices. HPH SCC and GCC members are implementing the report's recommendations through coordination by the Joint HPH Sector Cybersecurity Working Group.
- The Financial Services SCC established the International Committee to explore and analyze global financial regulatory, legislative, and judicial activity, with emphasis on understanding the interaction with U.S. domestic financial law, regulation, guidance, and proposals. The committee collaborated with the U.S. Department of the Treasury to develop mitigation principles for cyberattacks targeting the global financial system.

SECURITY OF SOFT TARGETS AND CROWDED PLACES

The cornerstone of our successful democracy is an open society that provides the means to freely engage in a number of activities without fear of harm. The engine of our economy is fueled by businesses of all disciplines, and those within the Commercial Facilities and Transportation Sectors play an integral role in our daily lives. The phrase "soft targets and crowded places" refers to locations or environments that are generally accessible to the general public and, as befits the nature of their purpose, do not incorporate significant security measures.

Terrorists and other extremist actors have identified such locations as prime targets, vulnerable to low-sophistication tactics that entail few observable indicators. Several high-profile attacks occurred in 2017: in Las Vegas, Nevada, a gunman fired on 22,000 people attending an open air music concert; in Northern Virginia, a gunman shot members of Congress at a public baseball field; in New York City, a man drove a rented truck onto a crowded park path; and in Charlottesville, Virginia, a man rammed his vehicle into a crowd of protestors. This trend underscores the importance of DHS's continuing efforts to work closely with public and private sector partners to identify innovative means by which the evolving threat environment can be mitigated. In collaboration with its partners, NPPD is redefining how the critical infrastructure community demonstrably reduces the risk of a successful attack and directly supports visible efforts to enhance the security of soft targets and crowded places. The following are highlights of partners' efforts in 2017 to improve the security of soft targets and crowded places:

- In response to the 2015 attack by a former employee in San Bernardino, California, the Commercial Facilities Sector-Specific Agency (SSA) and SCC worked with the Society for Human Resource Management to address how human resource management can address terrorism, recognizing pathways to violence and preparing organizations to better understand violent behaviors.
- The American Car Rental Association, as an executive committee member of the Commercial Facilities SCC, began a collaborative effort with DHS and the Federal Bureau of Investigation (FBI) to identify and implement methods and processes to reduce the likelihood of rental vehicle use in terrorist attacks.
- The Commercial Facilities Sector hosted a workshop with over 40 public and private sector participants on social media's role in perpetrating attacks, identifying and mitigating threats, and responding to incidents.
- The Transportation Systems Sector collaborated with the Transportation Security Administration and NPPD to develop the *Public Area Security National Framework* for deterring and responding to attacks in public areas.
- The Federal Protective Service (FPS) developed a *Soft Targets/Crowded Places Concept of Operations and Guide to Protection Activities* for the Government Facilities Sector. The guide identifies 135 activities performed by FPS that support the protection of soft targets and crowded places and provides a methodology for integrating the activities in a comprehensive way to counter common methods of attack.
- NPPD continues to maintain a comprehensive Active Shooter Preparedness Program with resources to enhance preparedness and response to an incident. The program website was updated in 2017 to adapt to the changing threat environment and provides posters, pocket guides, booklets, and fact sheets in nine different languages. In addition, videos and templates are provided for enhancing the understanding of behavioral indicators of violence and developing effective emergency action plans.

NEW SUBSECTOR: ELECTION INFRASTRUCTURE

In January 2017, DHS designated election infrastructure as critical infrastructure and created the Election Infrastructure Subsector (EIS) under the Government Facilities Sector. The designation underscored the importance of this infrastructure and the elections it facilitates, enabled the formation of the SSA and coordinating councils, and guided contributions of Federal support to State and local election officials. The following are highlights of partners' efforts in 2017 to address critical infrastructure security and resilience efforts for election infrastructure:

- The Election Infrastructure SSA was established to provide a coordinating office to facilitate the development of the EIS partnership framework.
- The SSA worked with the newly formed Election Task Force to coordinate Federal partners to unify efforts to understand the threat, provide services and products to stakeholders, and ensure a representative and effective security-informed partnership.

- In conjunction with the U.S. Election Assistance Commission (EAC), the Election Infrastructure SSA led the establishment of an EIS GCC to provide a forum for Federal, State, and local officials to meet regularly and discuss strategic objectives and information-sharing protocols.
- Through a series of Election Critical Infrastructure Working Group meetings over the summer of 2017, the Election Infrastructure SSA worked with the EAC, the National Association of Secretaries of State, and the National Association of State Election Directors to identify and invite key organizations to participate in the developing partnership. The working group finalized a GCC charter and initiated the development of information sharing protocols and EIS strategic goals and objectives.
- The Election Infrastructure SSA initiated security clearance opportunities for State Chief Election Officials and select staff to enhance information sharing within the EIS partnership.

NEW CROSS-SECTOR WORKING GROUPS

Working groups leverage the CIPAC partnership structure to target specific issues or opportunities whose urgency requires more focus and depth, where a capability gap has been identified, and/or when devoting additional resources will accelerate critical infrastructure safety and security. In 2017, new working groups were established to address cross-sector priorities, such as investigating a national access and reentry process, the potential threats presented by increasing use of unmanned aerial systems (UAS), and potential solutions to address insider threats. The following are highlights of partners' efforts in 2017 to leverage CIPAC in conducting cross-sector working group initiatives:

- A CIPAC working group was established in 2017 to update the Joint National Priorities for Critical Infrastructure Security and Resilience. NPPD hosted an in-person working group session and subsequent teleconferences with participation from SCCs, GCCs, and cross-sector councils to incorporate feedback and inputs.
- The Emergency Services Sector established a cross-sector working group to develop the *Crisis Event Response and Recovery Access Framework*. The document provides State and local jurisdictions with best practices and a common process approach to help jurisdictions establish their own access programs.
- The UAS Security Working Group—led by NPPD and the Critical Infrastructure Cross-Sector Council—was established to identify solutions for reducing risk, develop training resources, use UAS technology to enhance security, and develop cross-sector policy recommendations.
- The Critical Infrastructure Vetting Working Group (CIVWG) was established to examine private sector personnel screening solutions incorporating Federal Government security data to mitigate insider threats. In 2017, the working group developed an informational document that evaluates key elements of screening solutions and compares models that could support and enhance access determinations of critical infrastructure owners and operators.

CROSS-SECTOR COLLABORATION AND COORDINATION

Critical infrastructure issues and interdependencies span across sectors, industries, jurisdictions, and geographical areas. The four cross-sector councils—Federal Senior Leadership Council (FSLC), Critical Infrastructure Cross-Sector Council, SLTTGCC, and RC3—regularly meet as independent bodies and convene bi-annually for Joint Meetings of the Cross-Sector Councils. ISACs and the National Council of ISACs are key contributors to joint partnership initiatives and efforts by enhancing the ability to share information effectively within and across sectors.
The following are highlights of these partners' efforts in 2017 to address prominent cross-sector issues such as regional coordination, cybersecurity, and healthcare resilience:

- The SLTTGCC published its *Communications, Outreach, and Marketing Strategy* to direct internal and external communication, share best practices to advise on security and resilience issues, and provide Council perspectives on national issues. The Council also established Regional Liaisons to serve as contacts for NPPD's Regional Offices.
- The Critical Infrastructure Cross-Sector Council convened in 2017 to discuss lessons learned and identify common themes in support of the Joint National Priorities, including providing National Cyber Incident Response Plan guidance to help organizations better identify cyberattacks and improving owners' and operators' access to critical infrastructure affected by emergencies.
- Practitioners and decision makers from across the critical infrastructure community—including planners, government officials, civil engineers, architects, and private sector owners and operators—convened in a workshop led by NPPD to discuss the increasing convergence of cyber and physical infrastructure systems. Participants discussed the emerging cyber–physical risk landscape, tools and guidance to mitigate risks, and application of those products.
- NPPD led a Regional Resilience Assessment Program project on healthcare supply chains in New York City that facilitated cross-sector information sharing, risk analysis, and partnership building among multiple critical infrastructure sectors, including the Communications, Energy, Healthcare and Public Health, Transportation Systems, and Water and Wastewater Systems Sectors.
- Chemical Sector partners hosted the 11th Annual DHS Chemical Security Summit to exchange information and best practices, train sector partners, strengthen public–private networks, and obtain updates on security regulations. In total, 534 attendees participated in the 2017 Summit, including 460 attending in person and 74 via webinar.
- The Water ISAC co-hosted power resilience workshops with the U.S. Environmental Protection Agency and utilities in the Dallas and Phoenix metropolitan areas to share best practices regarding energy-water sustainability and emergency response following power outages triggered by natural disasters and manmade incidents.
- The Food and Agriculture SSA established a diverse working group of food and agriculture and healthcare subject matter experts from the Federal Government, private industry, and academia to develop the pending National Biodefense Strategy.
- A Sector Partnership Maturity Model was implemented and piloted across the following sectors: Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; and Nuclear Reactors, Materials, and Waste. The model provides an effective mechanism to assess the effectiveness and maturity of the processes and practices associated with each sector's partnership structures.

EXERCISES AND PREPAREDNESS

Cross-sector exercises and summits provide opportunities for government and industry leaders to discuss challenges on a variety of topics, including information and intelligence sharing, operational coordination, emergency authorities and waivers, industry mutual assistance, and public and private collaboration. The following are highlights of partners' efforts in 2017 to leverage exercises and preparedness to promote information sharing, education, awareness, and cross-sector collaboration:

- The Critical Manufacturing SSA, in collaboration with the Shelby County, Tennessee, Office of Preparedness, conducted a cross-sector supply chain workshop in Memphis that focused on supply chain and transportation impacts resulting from a bridge disruption. Participants included 41 regional, State, local, and private sector stakeholders.

- The 2017 GridEx IV was the largest exercise of its kind, gathering more than 6,000 participants from industry, government agencies, and partners in Canada and Mexico to simulate a cyber–physical attack on electric and other critical infrastructure.
- Participants from 22 countries observed CyberGuard 2017, a weeklong exercise co-led by U.S. Cyber Command, DHS, and FBI.
- The Cyberstorm VI national-level cybersecurity exercise was developed throughout 2017 by partners across the critical infrastructure community, including the Communications, Critical Manufacturing, IT, and Transportation Systems Sectors.
- In 2017, over 5,200 critical infrastructure partners and stakeholders participated in 26 exercises conducted by NPPD. Major elements of the exercise scenarios included active shooter, cyberattacks, explosives, natural disasters, UASs, and vehicle ramming. In addition, NPPD created the Outdoor Events and Insider Threat Sector-Specific Tabletop Exercise Program to assist the critical infrastructure community in designing and executing their own tabletop exercises to meet the needs of their facilities and stakeholders as it pertains to hosting a public event and better mitigating the impacts of a potential insider attack, respectively.
- NPPD leads the comprehensive Active Shooter Preparedness Program to inform stakeholders of the actions that should be taken before, during, and after an active shooter incident to mitigate potential impacts and support rapid recovery. In 2017, NPPD expanded the program's outreach by conducting 61 workshops for more than 4,600 partners and stakeholders across the United States. In addition, the active shooter website received more than 500,000 views, and nearly 100,000 online courses were successfully completed.

INFORMATION SHARING

Much of the critical infrastructure in the United States is owned and operated by the private sector, yet governments collect intelligence on related threats. Public–private collaboration and partnerships are essential to delivering the right information into the right hands to manage risks, respond to incidents, and close any divide between industry's economic goals and the Federal Government's national security interests. The following are highlights of partners' efforts in 2017 to expand technological capabilities, open avenues to improve information sharing, create new sector-specific groups, and remove barriers to sharing classified information with industry:

- In coordination with the ESCC, DOE and the electric industry began a secure communications pilot program to explore how senior executives can quickly receive classified briefings from remote locations during a major event.
- During the 2017 RSA Conference, the Automotive, Communications, Financial Services, and Water ISACs held a panel discussion on best practices and a framework for understanding the opportunities and challenges of intelligence sharing.
- A new National Defense ISAC was officially established and added to the membership of the National Council of ISACs, with a mission to enhance the security and resilience of the Defense Industrial Base Sector and strategic partners.
- The Nuclear Reactors, Materials, and Waste SSA conducted quarterly classified threat briefings, providing relevant and actionable threat information for owners and operators to assess security posture in light of the evolving threat environment.
- The Engagement Working Group (EWG), led by NPPD, coordinated with critical infrastructure partners and stakeholders to prioritize and exchange emerging classified and unclassified threat information. In the Joint Meeting of the Cross-Sector Councils in December 2017, the DHS Office of Intelligence and Analysis (I&A) and the newly formed DHS Office of Countering Weapons of Mass Destruction led EWG discussions regarding potential risk mitigation solutions for partners and stakeholders.

- NPPD, in coordination with I&A, developed a memorandum of understanding to provide classified briefings on a quarterly basis to public and private sector stakeholders across the country by leveraging fusion centers' capabilities for secure video teleconferences (SVTC). Leaders from the SLTTGCC, RC3, and National Council of ISACs collaborated with NPPD on developing operating procedures for SVTC.
- The Classified Intelligence Forum (CIF), co-chaired by DHS I&A and NPPD, conducted bi-weekly classified engagements that provided classified intelligence analytic products to cleared private sector members for their feedback and input. 2017 CIF engagements included participation from several critical infrastructure sectors, ISACs, SLTT intelligence agencies, and the Homeland Security Council.
- Throughout 2017, Homeland Security Information Network – Critical Infrastructure (HSIN-CI) provided 10,000 new products to almost 22,000 registered partners (a 19% increase in registered users). In addition, 35,000 partners participated in 2,550 webinars hosted by HSIN-CI users. During this time, HSIN-CI shared timely information with partners during 12 incidents, engaged in National Level Reporting and exercises, and produced a hurricane dashboard that will be available to SSAs for future incident use.

FOR ADDITIONAL INFORMATION

To learn more about CIPAC, the national partnership structure, or the 2017 highlights, please contact NPPD at CIPAC@dhs.gov or visit www.dhs.gov/cipac.

Homeland
Security