NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Quarterly Business Meeting
March 14, 2023

CALL TO ORDER, SWEARING IN, AND OPENING REMARKS

Ms. Erin McJeon, Cybersecurity and Infrastructure Security Agency (CISA) and Designated Federal Officer (DFO) for the President's National Infrastructure Advisory Council (NIAC), called the March 2023 NIAC Quarterly Business Meeting to order. She informed attendees that the NIAC is a Federal advisory committee, governed by the *Federal Advisory Committee Act* . As such, the meeting was open to the public. She noted that written comments would be accepted following the procedures outlined in the meeting's Federal Register Notice. The one public comment received would be addressed later in the meeting. Following roll call of members present in the room and on the telephone, Ms. McJeon turned the meeting over to the NIAC Chair, Mr. Adebayo Ogunlesi.

Mr. Adebayo Ogunlesi, Global Infrastructure Partners, thanked all those in attendance and especially the members of the Cross-Cutting Policy Challenges Subcommittee for their hard work. He expressed his hope that the NIAC would have a fruitful and worthwhile discussion about the report. He then welcomed Dr. Liz Sherwood-Randall, Assistant to the President, Homeland Security Advisor, and Deputy National Security Advisor, who gave opening remarks.

Dr. Sherwood-Randall welcomed and thanked all attendees and the Subcommittee for the work accomplished in completing the *Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement* report draft in rapid time to reflect the urgency of the issue. Dr. Sherwood-Randall then swore in three NIAC members: Ms. Christine Fox, Johns Hopkins Applied Physics Lab; Mr. David Gadis, DC Water; and Mr. Michael Hayford, NCR Corporation.

Dr. Sherwood-Randall stated that the resilience of critical infrastructure remains a high priority for the President, noting recent legislation like the *Bipartisan Infrastructure Law* and the *Inflation Reduction Act* which enhances economic competitiveness, addresses the climate crisis, and enables us to make our infrastructure more efficient, secure, and resilient. However, she said much work is still needed. Dr. Sherwood-Randall cited a current example of the historic atmospheric river events in California that have challenged our aging infrastructure. Whether we face extreme weather events or deliberate attacks, Dr. Sherwood-Randall emphasized we need to be more ready, resilient, and prepared to recover more quickly because of the impacts on our communities and economy.

Dr. Sherwood-Randall noted that the Federal Energy Regulatory Commission has tasked the North American Electric Reliability Corporation with reviewing the physical security standards at bulk power system substations. She highlighted that the increased recent substation attacks are an example of an evolving threat to our critical infrastructure that leads to the question of whether the government should continue with voluntary standards or transition to mandatory standards.

Dr. Sherwood-Randall advised that the Biden Administration remains committed to improving the nation's cybersecurity and has released the country's national cybersecurity strategy on March 2, 2023. Dr. Sherwood-Randall highlighted two fundamental shifts made by the new national cybersecurity strategy. The first shift involves rebalancing the responsibility of defending cyberspace away from small businesses and local governments and toward organizations that are best positioned to reduce risk. The second shift involves realigning incentives to favor long-term investments in a more resilient future. These two fundamental shifts will be advanced across five pillars:

1. Defend our critical infrastructure.
2. Disrupt and dismantle threat actors using all the instruments of national power to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.
3. Shape market forces to drive security and resilience.
4. Continue to invest in a resilient future through strategic investments and coordinated collaborative actions.
5. Forge international partnerships to pursue shared goals by seeking a world where responsible State behavior in cyberspace is expected and rewarded, and where irresponsible behavior is isolated and costly.

Dr. Sherwood-Randall shared that she and Ms. Caitlin Durkovich, Special Assistant to the President and Deputy Homeland Security Advisor for Resilience and Response, are reviewing the nation's critical infrastructure policy. Once the Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement draft report is finalized, it will provide valuable input to completion of policy reviews, promulgation of new guidance, and updates to Presidential Policy Directive (PPD)-21. She also noted that she and Ms. Durkovich are working to ensure that recommendations from the NIAC are translated into action and that this relationship between the government and the industry is a two-way street.

Mr. Ogunlesi thanked Dr. Sherwood-Randall for her comments and expressed his confidence and support for the Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement draft report. Mr. Ogunlesi invited Mr. Nitin Natarajan to address the NIAC.

Mr. Nitin Natarajan, Deputy Director of CISA expressed his excitement to hear from the Cross-Cutting Subcommittee on the short-term study. He shared that CISA would like to shift the paradigm of how government and industry work together to one of persistent collaboration as opposed to the current state of the government-industry relationship which is more episodic. He noted that the questions the Cross-Cutting Subcommittee was seeking to answer truly get to the heart of this goal and noted that the government-industry partnership should be finely tuned and constantly reevaluated. Mr. Natarajan thanked Mr. Ogunlesi, Ms. Maria Lehman, and the three subcommittee chairs for their leadership.

FINAL REPORT OF CROSS-CUTTING INFRASTRUCTURE POLICY CHALLENGES SUBCOMMITTEE

Mr. Ogunlesi turned the floor over to Mr. Manu Asthana, CEO of PJM Interconnection and Chair of the Cross-Cutting Infrastructure Policy Challenges Subcommittee (Cross-Cutting Subcommittee), who joined the conference by telephone. Mr. Asthana said he was honored to Chair the Cross-Cutting Subcommittee and promised to guide everyone through the report. He

acknowledged the work and input received from fellow subcommittee members, who included: Mr. Alan Armstrong, Williams Inc.; Mr. Joshua Descant, REV/REV Business; Mr. Hayford; Ms. Connie Lau, Hawaiian Electric Industries (Former); Mr. Pasquale Romano, ChargePoint; Dr. Conrad Vial, Sutter Health; Dr. Sadek Wahba, I Squared Capital; Mr. Christopher Wiernicki, American Bureau of Shipping; Mr. Craig Glazer, PJM; Mr. Dan Antilley, NCR Corporation; Mr. K.N. Gunalan, AECOM; and Ms. Jamey Barbas, New York State Thruway Authority.

Mr. Asthana noted that the Cross-Cutting Subcommittee's draft report, titled *Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement*, was the work of the entire Cross-Cutting Subcommittee, whose members gave extensive ideas and feedback throughout the six-week process. He also noted that the draft was given to the full NIAC to ask members for their feedback, both by inviting them to join a Cross-Cutting Subcommittee meeting and encouraging them to give written feedback.

In addition, he thanked Ms. Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technologies, and Ms. Jennifer Pedersen, Deputy Assistant Director for the National Risk Management Center at CISA, both of whom gave informative briefings to the Cross-Cutting Subcommittee. Lastly, he thanked Ms. Celinda Moening and Ms. McJeon, NIAC Alternate DFO (ADFO) and DFO, for their coordination throughout the process. The Cross-Cutting Subcommittee agreed upon nine barriers to cross-sector collaboration and ten recommendations to the President. Mr. Asthana turned the floor to Mr. Glazer, Cross-Cutting Subcommittee Member, to summarize the report.

Mr. Glazer highlighted the three main sections of the report, which included the Barriers to Cross-Sector Collaboration across the Sectors, Recommendations, and Voluntary or Mandatory Critical Infrastructure Standards. He emphasized the diversity of the subcommittee members; they each represented vastly different sectors that either manage critical infrastructure or rely on critical infrastructure through the supply chain. Because of the varying experiences and responses from each member, the subcommittee was able to identify common themes throughout their responses that led to the barriers and recommendations. As identified in the report's introduction, Mr. Glazer first wanted to define the word "collaboration." Collaboration encompassed the following: collaboration on infrastructure resilience and security among sectors within the private sector; collaboration of those sectors with Federal, state, and local governments; and collaboration between government, the private sector, and academic institutions.

Mr. Glazer pointed out a few of the barriers identified in the report, which included the following:

1. Lack of clarity, decision-making and command between Federal, state, and local governments in coordinating operations in emergency situations. He cited Hurricane Katrina and personal protective equipment distribution as examples.
2. Impact of time-sensitive interdependencies between sectors. He underscored sectors' awareness of cross-sector interdependencies and collaboration. For example, the electricity sector relies on the communication and water sectors, which in turn heavily depend on the electric sector. Therefore, disruptions in one sector directly impact other sectors' operations.
3. Lack of outcome-based goals to secure critical infrastructure.

4. Lack of cross-sector skills training and workforce development across sectors. He highlighted cross-sector skills training because it allows people to engage and understand the nature of other industries.
5. Information sharing on threats, both cyber and physical, with the Federal government.

Second, he emphasized a few of the specific, concrete recommendations provided in the report, including the following:

1. Need for the Federal government to administer cross-sector drilling exercises so that each sector would understand the impact and learn how to communicate with each other in case of an emergency, using GridEx as an example.
2. Need for more engagement from vulnerable communities, such as tribal and low-income communities, to be involved in early preparations for a potential disaster event.
3. Need for common cause failure analyses that are focused on supply chain vulnerabilities, in which multiple components of the system may fail due to a single common cause.
4. Need to prioritize standard setting in the areas of patch management and threat modeling that impact the performance of critical infrastructure sectors. Reliable and secure software is critical to critical infrastructure sectors' operations. Third-Party Certifications of the equipment that critical infrastructure owners and operators are buying within the supply chain could be piloted and existing government standards on procurement could be expanded.

Mr. Glazer then moved onto the topic of voluntary versus mandatory standards as detailed in the report. He noted that all the subcommittee members individually agreed that implementing mandatory standards is best in key areas, such as in cybersecurity. He also emphasized that the mandatory standards must be outcome-based, encouraging more focus on the "what" rather than "how" industry reaches that standard. Mr. Glazer then asked if the other subcommittee members would like to add anything.

On the topic of voluntary versus mandatory standards, Ms. Lau observed that the natural inclination for the private sector is to want less regulation and pointed out the significance of all subcommittee members favoring more regulation. She noted that with all the good work that is happening in the cybersecurity sector and where cyber meets other sectors, we need minimal required regulation. She also emphasized the importance of receiving input from private industry when creating the standards so that private industry feels included in the government's decision to regulate.

Dr. Sherwood-Randall asked the subcommittee members to guide the government in the best way to introduce mandatory standards so that this is received as a partnership to strengthen our national posture against all hazards. Ms. Lau recommended convening the government for cross-sector drilling to show the full supply chain impact to a given incident. When sectors see that they are involved in any resulting issues, they will understand the need for some regulation.

Likewise, Mr. Armstrong said that increasing understanding among the sectors is critical to having them on board for advanced regulation. As an example, he said within the pipeline industry, service providers that work with critical industries need to meet certain standards to provide services. Having the customer dictate their utility standards to the service provider is a way to ensure standards will be met. When providing a service, there should be a certification for

critical infrastructure owners and operators to meet. He also warned against applying regulatory mandates too broadly.

Mr. Wiernicki echoed Mr. Armstrong's point and suggested that standards and training should go together. He said all defense contractors are required to obtain Computerized Maintenance Management System (CMMS) certifications in lieu of a voluntary National Industry Security Program, in addition to third-party industry standards like the International Organization for Standardization standards. He said there is always an opportunity to implement new standards and build on precedents.

Mr. Asthana reiterated the importance of prioritizing outcome-based standards that focus on the "what" instead of the "how," especially within vulnerable communities. Dr. Vial agreed and highlighted the opportunity to identify cross-sector metrics. When mandatory standards are applied, often those metrics focus on the new technology of the day instead of meaningful metrics that have been collected. He suggested having the mandatory standards focus instead on the metrics. He concluded that the report is a foundation to build on as opposed to prescriptive instructions.

Ms. Maria Lehman, GHD and NIAC Vice Chair, observed that the ASCE currently has 74 standards. However, many of these standards are prescriptive instead of performance based. Prescriptive standards prevent adapting to changes quickly. Our standards need increasingly to adapt to changes quickly considering the rate of climate change. She also highlighted the need for a national de facto standard that would provide a consistent framework across the sectors and discourage reinventing the wheel. Mr. Wiernicki agreed and added that standards across sectors must operate like a common shared language or a common playbook to encourage consistency.

Dr. Sherwood-Randall added to her original question, asking subcommittee members to provide tangible examples for how to implement the mandatory standards. Ms. Lau answered that the key to encouraging industry to be on board is having iterative standards that are updated with input from the private sector, especially because the areas of cyber and tech change constantly. She emphasized that this relationship cannot be "one and done." She appreciated Dr. Sherwood-Randall's language from her opening remarks indicating that the relationship between the government and the private sector is a two-way street, which would be important when establishing standards. She also emphasized the need for a process to understand what is feasible and implementable in the standard's timeframe.

Ms. Audrey Zibelman, Senior Advisor and Board Member, indicated the need for the standards to be appropriate and at a minimal cost to not burden small industries. Dr. Vial added that information-sharing and analysis centers are underutilized for cross-sector collaboration. However, as stated in the report, private industry must feel comfortable sharing its challenges, not just its successes. He suggested implementing a standard specifically for information sharing. Ms. Beverly Scott, Beverly Scott & Associates, advocated for incorporating these concepts discussed into the way that business is done at every level. She also thanked the subcommittee for calling out the importance of earning the public's trust by building up vulnerable communities and voices.

Ms. Durkovich thanked the subcommittee chair and members and echoed Dr. Sherwood-Randall's question, asking the members to provide more tangible standards. She gave the

examples of CMMS and the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards. She said that the government needs input from the private sector but asked how to obtain input from various sectors. Lastly, she highlighted the point mentioned previously regarding the importance of security for the threats we face and how it should be a regular part of business.

Mr. Glazer suggested avoiding the word "standard," which often comes with pushback, and replacing it with language like "procurement process" and "certificate" instead. Mr. Asthana called back to Mr. Armstrong's point that the standard must be a prerequisite to providing a service. Mr. Hayford, who comes from the information technology industry, said that those in his industry often do not know the other members in their supply chains. He stated that in today's world, if the service provider (e.g., Microsoft, Amazon Web Services (AWS), etc.) makes a change to their platform, the platform will be shut down for an hour or the amount of time it needs to be fixed. He stated the importance of knowing what will result from that shut-down and finding alternative options to continue work.

Mr. Wiernicki joined the standards conversation using the example of a management system. Each of the critical sectors have different management systems relating to cyber. To create a common management system with common standards and common language, he suggested collecting information from all 16 sectors and bringing it to CISA for the purpose of finding commonalities in terms of data sharing, closing vulnerability gaps, or facilitating trade recovery. Once the commonalities are identified, then the next steps will become part of the procurement process.

Ms. Deneen DeFiore, United Airlines, emphasized that many large tech companies are not held accountable for releasing quality software technology. Thus, the burden of compliance falls on users of their software, which includes critical infrastructure industries. All the sectors represented around the room, she said, rely on these large service providers which are not adequately regulated.

Dr. Sherwood-Randall gave an example where the Administration had to prepare for the possibility of a national rail strike that would impact many industries as a result. Fortunately, the rail strike did not happen, but she said the sectors would have been dramatically affected with all goods and services shutting down, which is an example of how a labor dispute could impact the entire nation. Ms. Lau noted that people across the country were generally unaware as to the impact the rail strike would have. She added to Ms. DeFiore's point, stating that it is important to identify critical providers to critical infrastructure and push the regulation down, using the example of banking regulators that review core banking systems down to the mid-size and smaller banks.

Mr. Wiernicki agreed with Ms. DeFiore's position on accountability and software providers and recommended adding software issues to the subcommittee's recommendation. Mr. Armstrong highlighted the section in the report that suggests addressing all critical infrastructure suppliers in the supply chain regarding standards. He suggested pulling this point into the recommendations section of the report. Dr. Norma Jean Mattei, University of New Orleans, asked how the mandatory standards may be adjusted as needed, to which Mr. Wiernicki answered the purpose of having outcome-based standards is that it allows more flexibility for achieving the standard.

Mr. Natarajan noted his appreciation for the preceding comments and inquired, on the broad topics of secure-by-design and secure-by-default, how we prioritize areas to focus on and what a cross-sector solution looks like. He expressed his interest in deriving the greatest gains for all industries through a tiered and prioritized approach. Mr. Hayford replied and stated that first we need to know which software is critical and which is not for critical infrastructure, and then we need to build it from the bottom-up.

Ms. Fox appreciated the suggestion to expand GridEx for a cross-sector solution experiment. She suggested applying different standards in exercise scenarios. Ms. Madhu Beriwal, Innovative Emergency Management, noted that there are critical points where industries interact. Standards must be applied to the intersections between sectors. Ms. Beriwal stated that to create pertinent common standards, we need an architecture of expected performance outcomes that are important from a management perspective and a framework for decision making. For example, the Incident Command System took years to build their standardized approach for coordinating multi-sector emergency responses. Dr. Vial agreed that focusing on outcome-based approach that commands iteration gives people a sense of authenticity and co-creation.

Mr. Asthana added a final point to the discussion on the *Cross-Sector Collaboration to Protect Critical Infrastructure* report, encouraging members to separate recommendations for small changes from recommendations for large changes. He suggested that large or substantive additions might best be addressed through additional taskings in the future. Mr. Ogunlesi thanked everyone for their thoughts on the ideas discussed and hoped they would be helpful for government stakeholders. Then he shifted to the next agenda item—updates from the Water Security and Electrification Subcommittees.

UPDATES ON ADDITIONAL STUDY TOPICS

Dr. Mattei, Chair of the Water Security Subcommittee, provided an update of the Water Security Subcommittee's progress, which has culminated in weekly meetings and discussions on broad issues in water supply. She then named the members of the Water Security Subcommittee, who included: Ms. Camille Batiste, Archer Daniels Midland Company; Ms. Fox; Mr. Gadis; Ms. Clara Pratte, Strongbow Strategies; Mr. Jorge Ramirez, GCM Grosvenor; Ms. Patricia Sims, Drake State Community & Technical College; Mr. Vance Taylor, California Governor's Office of Emergency Services; and Damian Georgino, Womble Bond Dickinson.

Mr. Gil Quiniones, ComED and Chair of the Electrification Subcommittee stated that the Electrification Subcommittee's mission is to explore the most significant challenges and risks to the security and resilience of our nation's critical infrastructure posed by widespread electrification. He shared that the subcommittee is just beginning work and will report out in future meetings. Mr. Quiniones welcomed additional members to join the Electrification Subcommittee and named current members, who included: Mr. Armstrong; Mr. Asthana; Ms. Beriwal; Ms. DeFiore; Ms. Lau; Dr. Scott; Dr. Sims; Mr. Tony Thomas, Windstream Communications; Mr. Wiernicki; Ms. Zibelman; and nominees Mr. Thomas Klin, GHD; and Mr. David Quam, 56 Capital Partners.

PUBLIC COMMENT

Mr. Russell Branzell, President and CEO of the College of Healthcare Information Management Executives (CHIME), requested the NIAC recognize the needs of the healthcare/public health sector. He presented four main points for consideration, including the following:

1. Cybersecurity is imperative to national defense. Without a strong cyber posture in healthcare, strong national defense is impossible.
2. Cybersecurity, including ransomware, poses a direct threat to patient safety. Attacks against the healthcare sector have skyrocketed during the COVID-19 pandemic.
3. Healthcare is experiencing a dual pandemic stemming from workforce and economic pressures.
4. The healthcare sector needs more resources. The healthcare ecosystem is both target rich and resource poor.

COUNCIL DELIBERATION

Mr. Ogunlesi asked the NIAC to deliberate on any tweaks they would like made to the *Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement* report. Ms. Durkovich and several NIAC members requested amendments.

Ms. Durkovich acknowledged the need for additional forums to pursue cross-sector collaboration. Mr. Glazer agreed that the report can be amended to acknowledge the need for a forum, which will analyze issues going forward.

Ms. DeFiore requested to clarify the standards for operating system developers and vendors, rather than only having standards for end users, which Mr. Glazer acknowledged.

Ms. Pratte requested the addition of tribal governments in recommendation number three in the report, where the subtitle reads "Enhance Coordination Among Local, State and Federal Government Entities."

Ms. Lau requested that the typo in recommendation eight be corrected from CMMS to CMMC.

Dr. Mattei highlighted the need to support the technical workforce serving the public sector, given the hiring and retention challenges.

Ms. Durkovich suggested providing a few tangible examples of existing performance-based standards to support the recommendation for the development of additional standards, which Mr. Glazer acknowledged.

Mr. Ogunlesi asked the members to raise their hands to show who is in favor and who is opposed to the report, as amended. All were in favor, and none opposed. The *Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement* was adopted, as amended.

CONCLUDING REMARKS AND ADJOURNMENT

The March QBM concluded with Ms. Durkovich acknowledging the work of the Chair and Vice Chair and thanking the Cross-Cutting Subcommittee for their work. Ms. Durkovich reiterated highlights from the conversation on moving from voluntary to mandatory standards, especially in cross-cutting sectors. Ms. Durkovich addressed the recommendations and said she was in favor of conducting more testing and exercises; in fact, one of her directorate's responsibilities at the National Security Council is running exercises with the Federal Emergency Management Agency, where she found the exercises immensely valuable. She also indicated that the White House would work to ensure that the subcommittee's recommendations result in action. Ms. Durkovich discussed convening the Homeland and Critical Infrastructure Response Interagency Policy Committee to review the recommendations, which will help establish who has the responsibility to take action, and to report the findings in June, with a possible request for additional work.

Mr. Ogunlesi echoed Ms. Durkovich's sentiments, and he thanked everyone for the work they did to adopt the *Cross-Sector Collaboration to Protect Critical Infrastructure: Barriers and Recommendations for Improvement* report, stating his satisfaction with the contributions of the NIAC members who were present and on the phone. He concluded with wishing everyone safe travels.

MARCH 14, 2023 NIAC QBM PARTICIPANTS LIST

NAME	ORGANIZATION
NIAC MEMBERS	
Mr. Adebayo Ogunlesi	Global Infrastructure Partners
Ms. Maria Lehman	GHD
Mr. Alan Armstrong	Williams, Inc.
Mr. Manu Asthana	PJM Interconnection
Ms. Camille Batiste	Archer Daniels Midland
Ms. Madhu Beriwal	Innovative Emergency Management
Ms. Deneen DeFiore	United Airlines
Mr. Joshua Descant	REV/REV Business
Ms. Christine Fox	Johns Hopkins University APL
Mr. David Gadis	DC Water
Mr. Michael Hayford	NCR Corporation
Ms. Constance Lau	Hawaiian Electric Industries (Former)
Dr. Norma Jean Mattei	University of New Orleans
Ms. Clara Lee Pratte	Strongbow Strategies
Mr. Gil Quiniones	ComEd
Mr. Jorge Ramirez	GCM Grosvenor
Mr. Pasquale Romano	ChargePoint
Ms. Beverly Scott	Beverly Scott & Associates
Ms. Patricia Sims	Drake State Community & Technical College
Mr. Luis Vance Taylor	California Governor's Office of Emergency Services
Mr. Anthony Thomas	Windstream Communications
Dr. Conrad Vial	Sutter Health
Dr. Sadek Wahba	I Squared Capital
Mr. Christopher Wiernicki	American Bureau of Shipping
Ms. Audrey Zibelman	Senior Advisor and Board Member
GOVERNMENT PARTICIPANTS	
Dr. Liz Sherwood-Randall	Executive Office of the President
Ms. Caitlin Durkovich	National Security Council
Mr. Jason Averill	National Security Council
Mr. Jason Tama	National Security Council
Ms. Parry VanLandingham	National Security Council
Mr. Nitin Natarajan	Cybersecurity and Infrastructure Security Agency
Ms. Alaina Clark	Cybersecurity and Infrastructure Security Agency
Mr. Trent Frazier	Cybersecurity and Infrastructure Security Agency
Ms. Elizabeth Gauthier	Cybersecurity and Infrastructure Security Agency
Ms. Erin McJeon	Cybersecurity and Infrastructure Security Agency
Ms. Celinda Moening	Cybersecurity and Infrastructure Security Agency
Ms. Leilani Coates	Cybersecurity and Infrastructure Security Agency
Ms. Jamie Fleece	Cybersecurity and Infrastructure Security Agency

Ms. Deirdre Gallop-Anderson	Cybersecurity and Infrastructure Security Agency
Ms. Marilyn Stackhouse	Cybersecurity and Infrastructure Security Agency

NIAC POINTS OF CONTACT

Mr. Dan Antilley	NCR Corporation
Ms. Joanna Baltes	ComEd
Mr. Simon Boyce	Strongbow Strategies
Ms. Mary Burke	NCR Corporation
Ms. Amanda Mertens Campbell	Williams, Inc.
Ms. Felicia Davis	Windstream Communications
Ms. Caryl Driscoll	Williams, Inc
Ms. Emily Feenstra	American Society for Civil Engineers
Mr. Trent Fellers	Windstream Communications
Mr. Bobby Fraser	United Airlines
Mr. Craig Glazer	PJM Interconnections
Ms. Lili Hasse	Global Infrastructure Partners
Mr. Max Leichtman	ComEd
Ms. Nellie Maldonado	ChargePoint
Dr. Toni Matheny	Johns Hopkins University APL
Ms. Margaret McDonagh	ComEd
Mr. Tom Murdock	Johns Hopkins University APL
Mr. Rob Nichols	Johns Hopkins University APL
Mr. David Quam	Drake State Community and Technical College
Ms. Lisa Salmon	PJM Interconnection
Mr. William Smith	NCR Corporation
Ms. Tara Template	REV/REV Business
Ms. Hannah Weber	Global Infrastructure Partners
Ms. Susan Wise	I Squared Capital

CONTRACTOR SUPPORT

Ms. Diamond Alexander	TekSynap Corporation
Mr. Stephen Arthur	TekSynap Corporation
Mr. John Finn	TekSynap Corporation
Mr. Garen Franklin	Edgesource Corporation
Ms. Jenna Harrity	Edgesource Corporation
Ms. Barbara Nowak	TekSynap Corporation
Ms. Nikita Sescoe	Edgesource Corporation

PUBLIC PARTICIPANTS AND MEDIA

Sara Amish	Western Governors Association
Chelsea Arnone	CHIME
Karin Athanas	TIC Council Americas
Jamey Barbas	New York State Thruway Authority
Russell Branzell	CHIME
Sara Friedman	Inside Cybersecurity
K.N. Gunalan	AECOM
Carol Haddock	Houston Public Works
Maggie O'Connell	Interstate Natural Gas Association of America
Christian Vasquez	CyberScoop