Quarterly Business Meeting

December 10, 2020

NIAC The President's National Infrastructure Advisory Council

Opening Remarks

NIAC The President's National Infrastructure Advisory Council

Actionable Cyber Intelligence:

An Executive-Led Collaborative Model

December 10, 2020

NIAC The President's National Infrastructure Advisory Council

Agenda

- NSC Guidance
- Foundational Elements
- Distinct Role and Capabilities
- Requirements
- Challenges
- Recommendations
- Questions

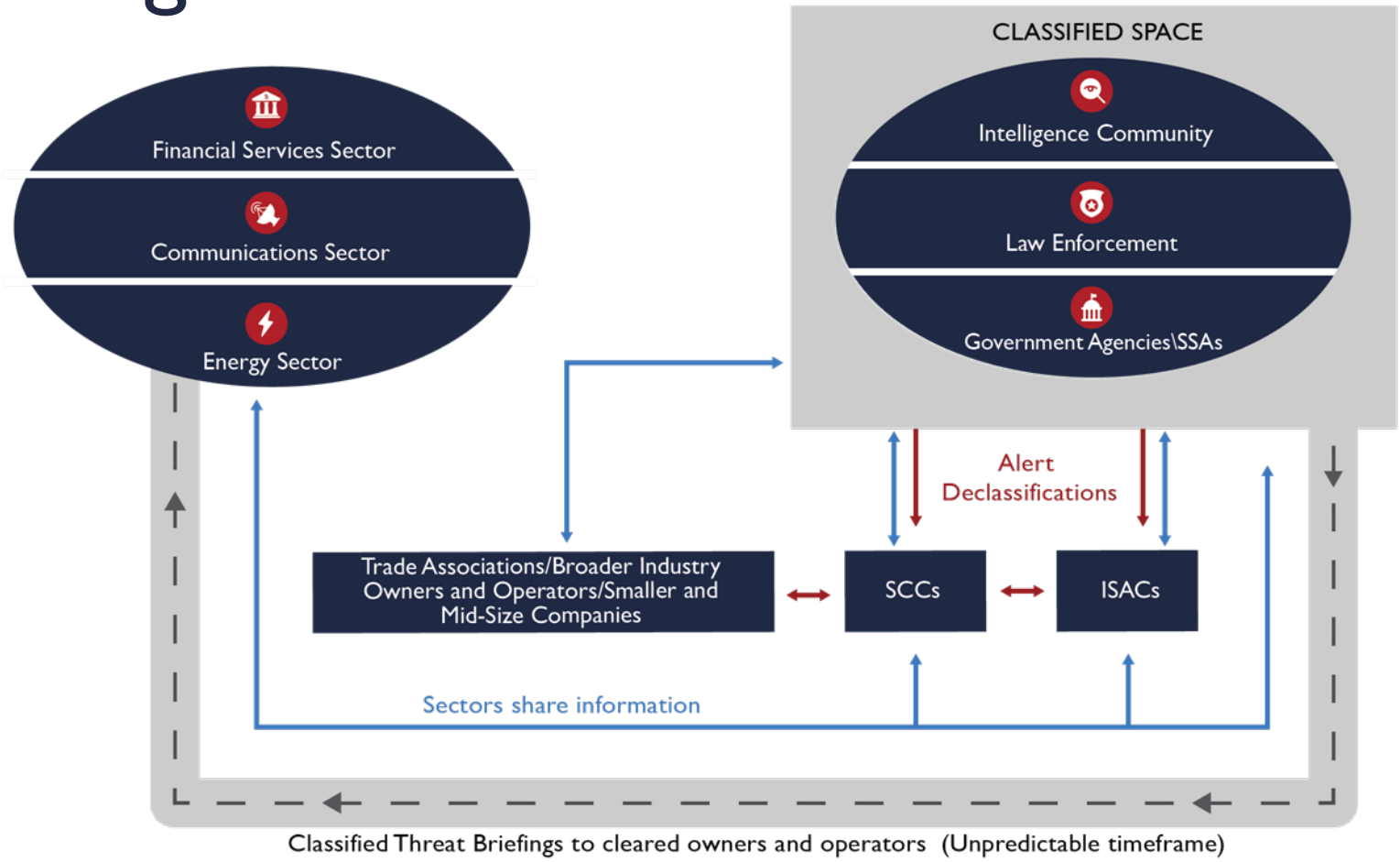
NSC Guidance

- Conduct follow-on analysis to:
  1. Demonstrate the value provided by the NIAC's 2019 recommendation to establish a Critical Infrastructure Command Center (CICC)
  2. Identify challenges that must be addressed
  3. Recommend an approach to achieve CICC operational functionality

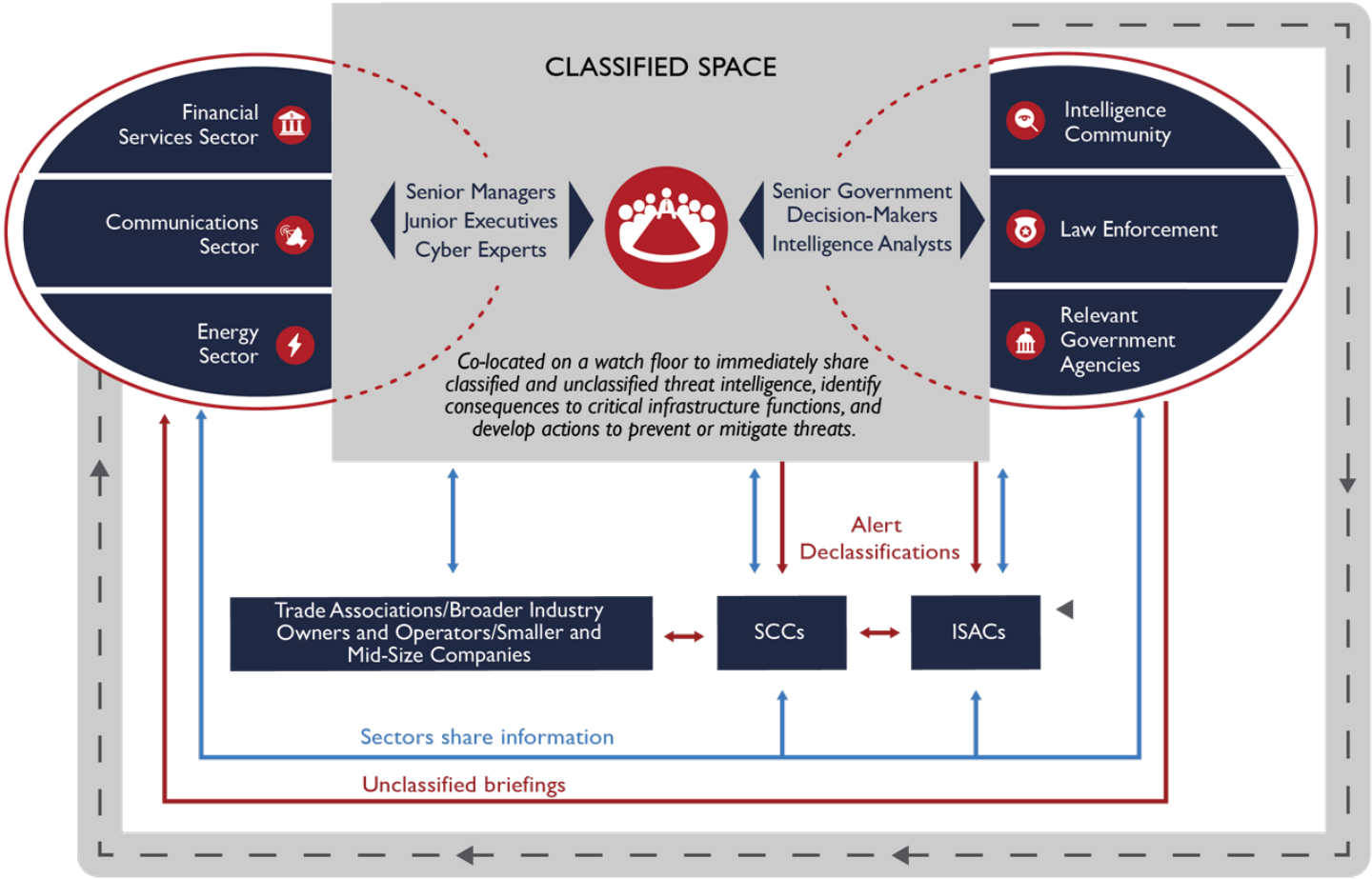
Foundational Elements

- CICC concept will not replace existing information sharing mechanisms, it will fill current operational gaps
- Must be private-sector led and have executive-level engagement
- Initial facility, staff, agreements, and operations can be rapidly implemented at the direction of private sector and government executives
- Value differentiator is operationalizing threat intelligence with recommended actions such as code, technology configurations, and remediation actions

Existing Public-Private Intelligence Sharing



CICC Concept Role in Relation to Existing Entities



Value Provided

- **Provide mitigating actions and tools** to help organizations reduce or eliminate risk to operations
- **Analyze threat intelligence to prioritize risks**, assess potential impact, and release code or tools to help organizations (including small- and medium-sized entities) make informed decisions
- **Accelerate and improve response** to the most serious threats
- **Enrich intelligence** with private sector insights and context
- **Identify patterns across sectors** to improve response time, alerting, and coordination between public and private sector actions

CICC's Distinct Capabilities (1/5)

- **Provide real-time, direct collaboration between government intelligence analysts and experts from the private sector** to efficiently identify, analyze, and mitigate national security level threats to highly critical sectors, with oversight and engagement of senior managers from private sector and government.

CICC's Distinct Capabilities (2/5)

- **Develop innovative mitigation measures** by using the collective expertise of private sector CICC staff, government managers, and national experts to directly share with the broader critical infrastructure community (including ISACs and small and medium sized entities).

CICC's Distinct Capabilities (3/5)

- **Assess a threat or vulnerability's consequences to broader critical infrastructure sectors**, assist in issuing an alert that can be shared broadly, and share tools to help determine if the vulnerability is on a company's system.

CICC's Distinct Capabilities (4/5)

- **Monitor threat activity on infrastructure systems that could indicate targeting of a particular sector or device/system,** provide sector-specific insights to assess impacts to operations and supply chain, and inform appropriate government or company response.

CICC's Distinct Capabilities (5/5)

- **Allow the intelligence community (IC) to quickly share threats and intelligence with private companies** and enable the private sector to add valuable context to support improved intelligence collection.

Requirements to be Successful

- Co-located senior private sector managers, company cyber experts, government managers, and government intelligence analysts working side-by-side
- Ability to engage internal CICC staff and external expertise from National Labs, academia, vendors/service providers, etc. to rapidly develop, test, and disseminate mitigations and response actions based on the severity of the threat
- Government analysts with the mission and authority to collect intelligence on threats to privately owned critical infrastructure systems and make the private sector an explicit intelligence community customer

Challenges and Potential Barriers

- Participation and sharing agreements from the private sector, intelligence community, and other federal agencies
- A secure classified space and ability for companies to securely access their networks and conduct secure virtual calls
- Authorities to make the private sector an explicit intelligence community customer, allowing the intelligence community to share threats with private companies
- Lack of liability protection for private sector entities if they share cyber threat information

Recommendations (1/4)

- Direct the relevant federal agencies to support the private sector in rapidly standing up the CICC concept with the energy, financial services, and communications sectors:
  - Within 90 days the private sector will identify the executives who will lead execution of the CICC concept and establish governing criteria.
  - Within 120 days the CICC sector executives will identify and assign the necessary CICC staff from the private sector.
  - Within 90 days an appropriate venue to house the operational component will be identified and the necessary agreements put in place.

Recommendations (2/4)

- Direct the Intelligence Community and other relevant government agencies to identify and co-locate the required government staff counterparts to enable the direct coordination required by the CICC. This staff should be pulled from the Intelligence Community, Sector-Specific Agencies, and law enforcement.

Recommendations (3/4)

- Establish the appropriate authorities and mission for federal agencies to directly share intelligence with critical infrastructure companies, along with any other authorities required for the CICC concept to be fully successful.

Recommendations (4/4)

- Once the CICC concept is fully operational (within 180 days), the responsible executives should deliver a report to the NSC and the NIAC demonstrating how the distinct capabilities of the CICC have been achieved and the impact of the capabilities to date. The report should identify remaining gaps in resources, direction, or authorities.

Questions?

Appendix

Working Group Members

- **J. Rich Baich**, Chief Information Security Officer, AIG (Co-Chair)
- **William J. Fehrman**, President and CEO, Berkshire Hathaway Energy
- **Kevin Morley,** Manager, Federal Relations, American Water Works Association
- **Richard H. Ledgett, Jr.**, Senior Visiting Fellow, The MITRE Corporation (Co-Chair)
- **Ola Sage**, Founder and CEO, CyberRx; Former IT SCC Chair
- **Michael J. Wallace**, Former Vice Chairman and COO, Constellation Energy

Working Group Support

- **Jeffrey Baumgartner,** Senior Advisor, National Security and Resilience, Berkshire Hathaway Energy
- **Sam Chanoski,** Former Director, Threat Intelligence, E-ISAC, NERC
- **Kristina Dorville**, Head of Governance and Engagement, AIG
- **Charles Durant**, Former Director of National Security Policy and Resiliency Policy Advisor, Berkshire Hathaway Energy
- **Frank Honkus**, Associate Director, Intelligence Programs and CRISP Manager, E-ISAC

Organizations Interviewed

1. Australian Cyber Security Centre
2. Center for Cyber Security, University of Alabama at Birmingham
3. Cybersecurity and Infrastructure Security Agency
4. Cyberspace Solarium Commission
5. Cyber Threat Alliance
6. Cybersecurity Directorate, National Security Agency
7. Federal Bureau of Investigation
8. Financial Systemic Analysis and Resilience Center
9. Kansas Intelligence Fusion Center
10. President's National Security Telecommunications Advisory Committee
11. National Risk Management Center
12. United Kingdom National Cyber Security Centre
13. U.S. Coast Guard
14. U.S. Cyber Command
15. Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

Workforce and Talent Management Study

Study Update

December 10, 2020

NIAC The President's National Infrastructure Advisory Council

Agenda

- NSC Guidance
- Framing Questions
- Working Group Approach
- Initial Themes
- Discussion Questions

NSC Guidance

- Conduct an in-depth study on the challenges facing the critical infrastructure workforce and the risks to national security posed by a lack of skilled workers
  - First NIAC study to examine worker-readiness across critical infrastructure sectors
- Develop near-term and long-term recommendations to improve worker readiness to ensure the continuity of the Nation's critical infrastructure sectors
  - Focus on a limited set of critical sectors – Energy, Water and Wastewater Systems, Transportation Systems, Communications, Financial Services, and Healthcare and Public Health – but develop recommendations that could have applicability across all sectors

Framing Questions

1. What are the major trends or changes currently transforming the workforce? What steps need to be taken to prepare for these changes?
2. How do we ensure critical infrastructure workers have the skills needed to operate, repair, or restore infrastructure in an emergency and in steady state?
3. What are some of the ways to train and/or develop the needed skills in the existing workforce?
4. How can stakeholders shape the workforce and education systems to meet the demand for certain skillsets to operate critical infrastructure?

Working Group Approach

- Focused on Framing Questions
- Conducted 15 interviews and 3 panels to gather insights and information from industry leaders and experts
- Conducted in-depth research on key topics:
  - Documented current workforce landscape for each critical infrastructure sector identified
  - Summarized current workforce legislative activity in Congress
  - Analyzed relevant after-action reports for workforce development recommendations
- Convened a Study Group of critical infrastructure and workforce development policy experts to conduct research, interviews, and provide in-depth analysis

Initial Themes (1/4)

What are the *major trends or changes* currently transforming the workforce? What steps need to be taken to prepare for these changes?

- Increasing workforce demands outpace the ability to fill the need due to retirements, lack of awareness of existing career opportunities, and availability of qualified candidates.
- Cybersecurity and digital literacy are required to support technologically changing landscape of critical infrastructure.
  - Equitable access to affordable, secure, high-speed internet, training, transportation, and other wrap-around services is needed to support the development of the workforce of the future.
- Critical infrastructure jobs continue to lack the diversity and inclusivity needed to reflect the communities they serve.
- Qualified applicants can be deterred due to stringent federal hiring practices, which affects agencies' ability to hire essential workers supporting critical infrastructure.
- The ongoing pandemic has highlighted the need to address these systemic workforce challenges.

Initial Themes (2/4)

How do we ensure critical infrastructure workers have the *skills needed* to operate, repair, or restore infrastructure in an emergency and in steady state?

- A more coordinated approach to identifying, prioritizing, and developing cross-sectoral programs, policies, and practices to respond to national emergencies and meet the challenges of tomorrow is an economic and national security imperative.
- Better data, modeling, and forecasting tools are needed to help identify and anticipate necessary skills and match talent to workforce needs.
- Flexible mutual aid agreements offer a model for broader critical infrastructure support during an emergency, specifically ensuring worker readiness to respond in a disaster.
- Reciprocity of certification can promote worker mobility and transferable skills during steady state operations, offering an adaptable talent pipeline that supports workforce readiness at the local, regional, and national level.

Initial Themes (3/4)

What are some of the ways to train and/or develop the needed skills in *the existing workforce*?

- Apprenticeships remain one of the most efficient forms of job training and pipeline development.
  - More than 23,400 individual programs currently participate in the Department of Labor's Registered Apprenticeship Programs.
  - Companies also utilize Industry-Recognized Apprenticeship Programs (IRAPs).
- Clearly defined career roadmaps, baseline skills, and credentialing will help workers understand opportunities to advance their careers.
- Public-private rotations and temporary deployments are a valuable way to acquire new skills and gain experience working in different sectors.
- Companies must continue to invest in training their workforce to develop new skills to meet the changing technology landscape.

Initial Themes (4/4)

How can stakeholders shape the workforce and education systems to meet the demand for certain skillsets to operate critical infrastructure?

- Systemic change bolstered by supporting regulations, legislation, and incentivizes is necessary to drive targeted recruiting programs and diversity, equity, and inclusion initiatives to expand the talent pool and draw new communities into the critical infrastructure workforce.
- Treat the workforce development system as a continuum to promote life-long learning opportunities.
  - Build dedicated partnerships in the K-12 system to foster awareness of necessary skills and career opportunities.
  - Build systems capable of providing wrap-around services that allow workers to take advantage of training opportunities without incurring additional hardships.
  - Build partnerships between technical colleges and employers to identify the skills needed and to develop a talent pipeline.
- Regional "ecosystems" between educational institutions and potential employers help pair skills, workers, and jobs.

Discussion Questions

- Do the initial themes align with what you are experiencing in your sectors?
- Are there structured programs and initiatives that successfully address the challenges or trends in your sector?

Appendix

Prior Recommendation Analysis

- This is the first NIAC study to examine worker-readiness across critical infrastructure sectors
  - Prior efforts referenced workforce as part of a larger effort
- 28 workforce recommendations from 7 prior NIAC studies since 2006
  - Majority are related to cyber workforce or focused on a single sector

WG Interviews Conducted (1/3)

- **Suzi LeVine** and **Cami Feek**, Commissioner and Deputy Commissioner, Washington State Employment Security Department
- **Robert Dean**, Assistant Business Manager, International Brotherhood of Electrical Workers
- **Kristin Best** and **Sarah Tauber**, Transportation Security Agency
- **Dr. Aisha Francis**, Benjamin Franklin Institute of Technology
- **Joseph Carbone**, President and CEO, The Workplace

WG Interviews Conducted (2/3)

- **Phillip Washington** and **Joanne Peterson**, LA Metro
- **Freeman Hrabowski** and **Greg Simmons**, University of Maryland at Baltimore County
- **Mark Hagerott**, Chancellor, North Dakota University System
- **Benjamin Shaw**, Director of Government Security Programs, Salesforce
- **Mark Dubina**, Vice President of Security for the Tampa Port Authority

WG Interviews Conducted (3/3)

- **Al Hancock, Randy White,** and **Steve Wenke**, Dams Sector Coordinating Council
- **Rachel Havrelock**, Associate Professor of English, University of Illinois at Chicago
- **Rita Moss**, Chief Human Capital Officer, CISA
- **Russ Matthys** and **Mark Ray**, Public Works Departments, Minnesota
- **David Lacquement, Alexandra Friedman, and Edward Roback**, U.S. Department of the Treasury

WG Panels Conducted (1/2)

National Governors Association Panel

- **Mary Catherine Ott**, Legislative Director, Homeland Security & Public Safety Committee (HSPS)
- **Stephen Parker**, Legislative Director, Education & Workforce Committee
- **Daniel Lauf**, Program Director, Center for Best Practices
- **Rachael Stephens**, Director of the Workforce Development & Economic Policy, Center for Best Practices

Pacific Northwest Regional Panel

- **Matthew Morrison,** CEO of the Pacific Northwest Economic Region (PNWER)
- **Brandon Hardenbrook,** COO of PNWER
- **Paula Scalingi,** Executive Director of the Institute for Innovating Security and Resilience and President of The Scalingi Group, LLC

WG Panels Conducted (2/2)

Financial Services Panel

- **Ben Flatgard,** Executive Director for Cybersecurity, J.P. Morgan Chase & Co.
- **Matthew Goard**, Vice President for cyber partnerships and government engagement, Morgan Stanley
- **Kristin Royster**, Senior Vice President, Global Information Security (GIS) team, Bank of America
- **Murray Kenyon**, Vice President, Cybersecurity Partnership Executive in Information Security Services, U.S. Bank
- **Heather Hogsett**, Senior Vice President of Technology & Risk Strategy, BITS Division, Bank Policy Institute
- **Kristina Dorville**, Head of Governance and Engagement at AIG

Working Group Members

Beverly Scott, Ph.D., CEO, Beverly Scott Associates, LLC (Co-Chair)

Jan Allman, President, CEO, and General Manager, Marinette Marine Corporation (Co-Chair)

Georges Benjamin, M.D., Executive Director, American Public Health Association

Terry Boston, Former CEO, PJM Interconnection

Robert Carr, Founder and Former CEO, Heartland Payment Systems

Margaret Grayson, Consultant, E2M, LLC

George Hawkins, Former CEO and General Manger, DC Water

Reynold Hoover, Former Deputy Commander, U.S. Northern Command

Rhoda Mae Kerr, Fire Chief, City of Fort Lauderdale Fire Rescue

Keith Parker, President and CEO, Goodwill Industries of North Georgia

Study Group Members

Nathaniel Millsap, Director Of Industrial Security and Technology, Fincantieri Marinette Marine

Nat Smith, Legal Advisor, Introducing Youth to American Infrastructure, Inc.

Peter Burns, Chair of Audit Committee (ret.), CardConnect

Jack Clark, Executive Director, Transportation Learning Center

Turahn Dorsey, Foundation Fellow, Eastern Bank Charitable Foundation; Co-Founder, Change Agency, Ltd.

Joseph Kane, Senior Research Associate & Associate Fellow, The Brookings Institution

Nitin Natarajan, Director, E3/Sentinel

Glenda Scarbrough, HR Director, Pacific Gas & Electric

Ty Schieber, President & CEO of Clarity Enterprise Solutions, LLC

Eric Seleznow, Senior Advisor, Jobs for the Future

Katie Spiker, Director of Government Affairs, National Skills Coalition

Adie Tomer, Fellow, Metropolitan Policy Program, The Brookings Institution

Andy Van Kleunen, CEO, National Skills Coalition

Rebecca Winkel, Economic Policy Advisor, American Petroleum Inst.

Dr. Afia Zakiya, Group Leader, Policy & Humanity, Black Chicago Water Council

Closing Remarks

NIAC The President's National Infrastructure Advisory Council