Quarterly Business Meeting

September 17, 2020

NIAC The President's National Infrastructure Advisory Council

Opening Remarks

NIAC The President's National Infrastructure Advisory Council

Workforce and Talent Management Study

Study Update and Discussion

September 17, 2020

NIAC The President's National Infrastructure Advisory Council

Working Group Members

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

Jan Allman, CEO, Fincantieri Marinette Marine Corporation (Co-Chair)

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

William 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

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
- 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

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

Framing Questions

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

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

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

4. What are the major trends or changes that are or will transform the workforce? What steps need to be taken to prepare for these changes?

Study Approach and Path Forward

- Use panels, briefings, and alternative engagements quickly gather insights and information
- Form a Study Group of outside experts
- Conduct in-depth research into existing resources and best practices from sectors, governments, and academic institutions
- **Dec. 10**: provide initial insights and key themes
- **Anticipated study completion**: Q3 2021

Questions?

“How COVID-19 is Changing Critical Infrastructure” Panel

September 17, 2020

NIAC The President’s National Infrastructure Advisory Council

Moderator

- **Dr. Georges Benjamin**, Executive Director, American Public Health Association; NIAC Member

Panelists

- **Kathryn Condello**, Senior Director, National Security/Emergency Preparedness, Lumen (formerly Century Link)
- **Bob Kolasky**, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency
- **Robert Puentes**, President and CEO, Eno Center for Transportation

CICC Follow-On Analysis

Status Update and Discussion

September 17, 2020

NIAC The President's National Infrastructure Advisory Council

Agenda

- ▶Organizations Interviewed
- ▶Initial Themes
- ▶Key Milestones
- ▶Questions

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. National Risk Management Center
11. United Kingdom National Cyber Security Centre
12. U.S. Coast Guard
13. U.S. Cyber Command

Initial Themes (1/3)

- Current models do not have the real-time collaboration and direct information flows between government and industry personnel necessary to achieve the CICC's objective.

- The CICC's value will come from the ability to connect the dots between threat intelligence, the potential consequences to critical infrastructure, and the innovation delivered by the CICC operators.

- Co-locating analysts that have access to their own networks enables them to discuss and analyze information in real-time without ever having to exchange or transfer data.

Initial Themes (2/3)

- Most successful entities currently operate at the Top Secret/Sensitive Compartmented Information (TS/SCI) level with limited bureaucracy between the intelligence being analyzed and its recipients.
- Extended time required to anonymize and de-classify data at the federal level and share with private sector may reduce the information's value and effectiveness (e.g., can take 24 hours to months to complete process).
- The appropriate authorities do not exist today to fully enable the CICC to operate at its intended state.

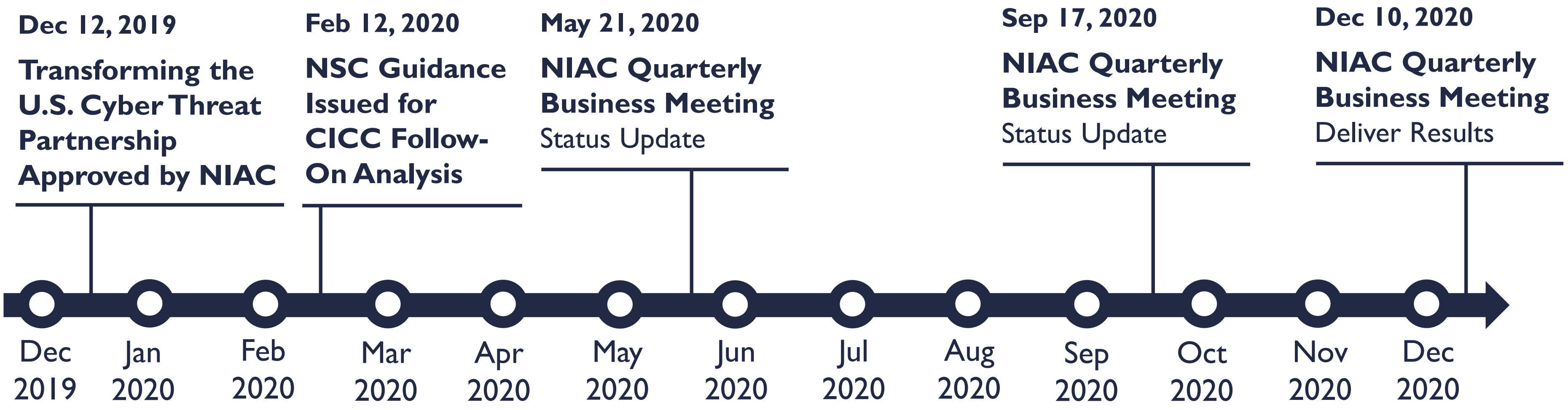
Initial Themes (3/3)

- Intelligence community is currently unable to share intelligence directly with private companies.
    - Both NIAC and Cyberspace Solarium Commission have recommended action
- Existing entities appear to rely on a patchwork of individual memorandums of agreement or understanding to engage with private sector on cyber collaboration and coordination, and there is not a standard agreement.
- Commitment is needed from the private sector to fund and provide the right level of resources to work in the CICC.

Discussion Questions

- What value does the CICC need to provide for the private sector to commit resources and personnel to the CICC?
- What concerns or issues would need to be addressed for you to participate?

Milestones



Dec 12, 2019
Transforming the U.S. Cyber Threat Partnership Approved by NIAC

Feb 12, 2020
NSC Guidance Issued for CICC Follow-On Analysis

May 21, 2020
NIAC Quarterly Business Meeting
Status Update

Sep 17, 2020
NIAC Quarterly Business Meeting
Status Update

Dec 10, 2020
NIAC Quarterly Business Meeting
Deliver Results

Dec 2019
Jan 2020
Feb 2020
Mar 2020
Apr 2020
May 2020
Jun 2020
Jul 2020
Aug 2020
Sep 2020
Oct 2020
Nov 2020
Dec 2020

Questions?

Appendix

NSC Guidance and Study Approach

- **Guidance:** Conduct follow-on analysis to:
  1. Demonstrate the value the CICC could provide
  2. Identify challenges that must be addressed
  3. Recommend an approach to achieve CICC operational functionality
- **Approach**: NIAC's 6-Member Working Group will:
  - Conduct briefings with key organizations
  - Conduct interviews with senior leaders in government and industry
  - Supplement interviews and briefings with focused research
  - Conduct work sessions to identify key themes and ultimately develop recommendations

Working Group Members

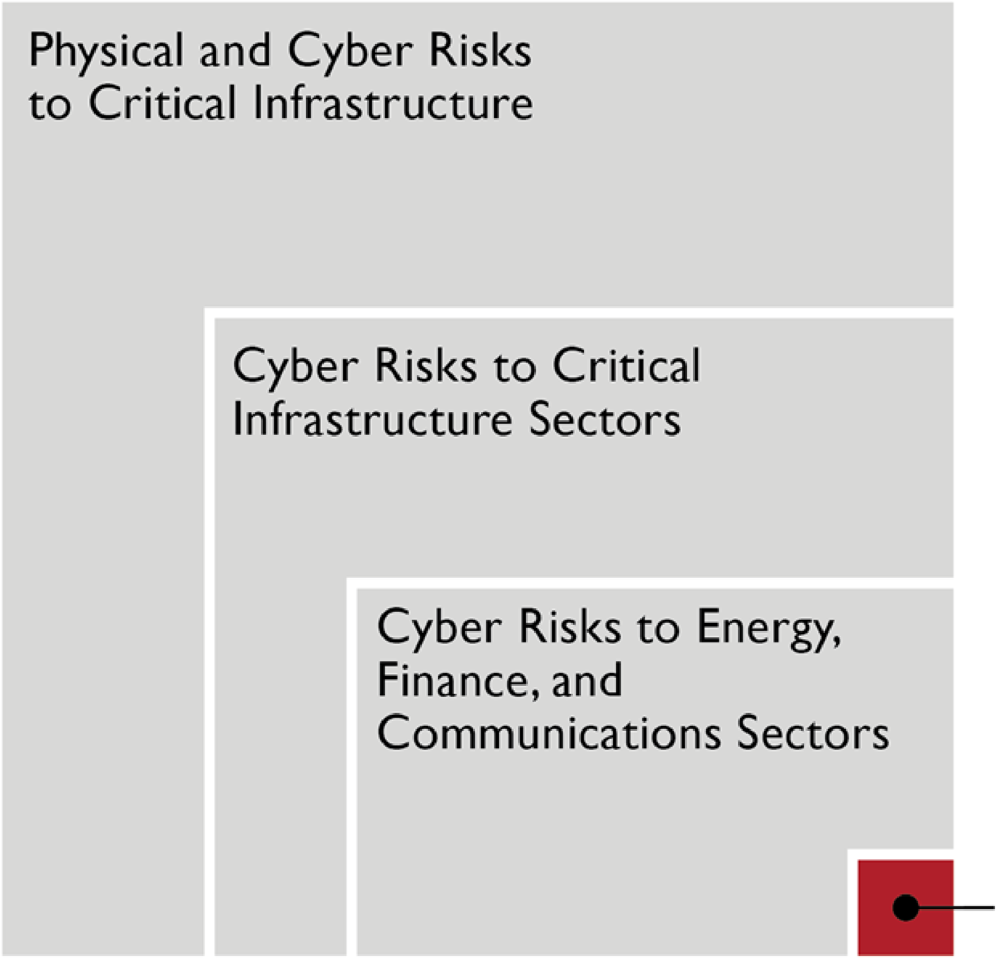
- **J. Rich Baich**, Chief Information Security Officer, AIG (Co-Chair)
- **William J. Fehrman**, President and CEO, Berkshire Hathaway Energy
- **Kevin Morley,** Manager, Federal Relations, American Water Works Association
- **Richard H. Ledgett, Jr**., Former Deputy Director of the National Security Agency (Co-Chair)
- **Ola Sage**, Founder and CEO, CyberRx
- **Michael J. Wallace**, Former Vice Chairman and COO, Constellation Energy

Working Group Support

- **Frank Honkus**, Associate Director, Intelligence Programs and CRISP Manager, E-ISAC
- **Kristina Dorville**, Head of Governance and Engagement, AIG
- **Charles Durant**, Director of National Security Policy and Resiliency Policy Advisor, Berkshire Hathaway Energy

Relevant Background from the 2019 Transforming the U.S. Cyber Threat Partnership Study

2019 Study Scope



Physical and Cyber Risks to Critical Infrastructure

Cyber Risks to Critical Infrastructure Sectors

Cyber Risks to Energy, Finance, and Communications Sectors

Limited Study Scope

Cyber Risks to Entities with National Security Implications

See 2019 report page: 4

Recommendations

FOUR STRATEGIES TO RESPOND TO CATASTROPHIC CYBER RISKS

Make Cyber Intelligence Actionable

Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission

Modernize Legal Authorities to Improve Cyber Defense

Secure the Supply Chain of Sensitive Components

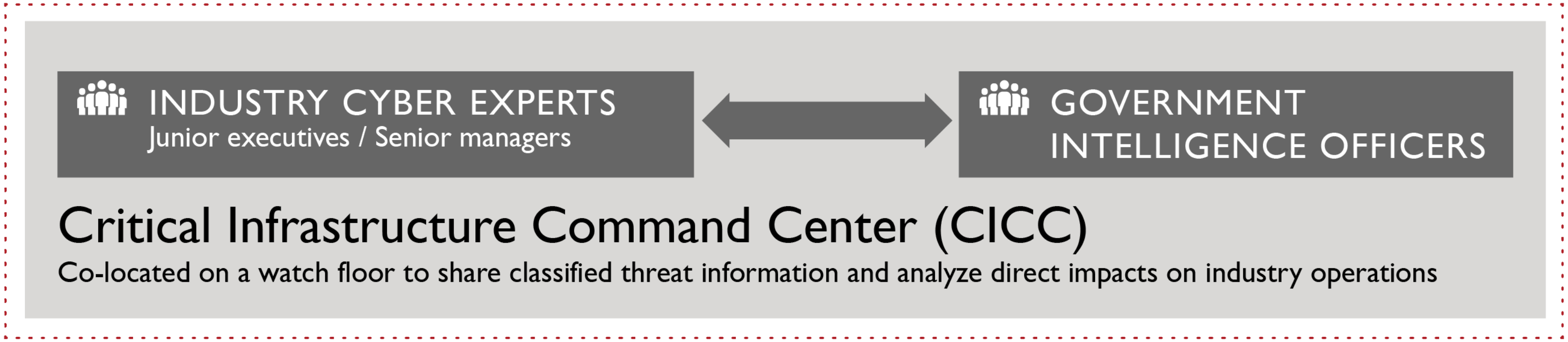
Make Cyber Intelligence Actionable

1. **Establish the Critical Infrastructure Command Center** (CICC) to improve the real-time sharing and processing of private and public data including classified information between government intelligence analysts, cyber experts from companies at greatest risk, and key government agencies.

See 2019 report page: 8

Make Cyber Intelligence Actionable

URGENT ACTION



INDUSTRY CYBER EXPERTS

Junior executives / Senior managers

GOVERNMENT INTELLIGENCE OFFICERS

Critical Infrastructure Command Center (CICC)

Co-located on a watch floor to share classified threat information and analyze direct impacts on industry operations

Make Cyber Intelligence Actionable

2. **Direct the Intelligence Community to raise the priority** of collecting and disseminating information on efforts by nation-states to exploit, deny, or attack U.S. critical infrastructure.
3. **Conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to CEOs** within the energy, communications, and financial companies to reinforce the compelling case for action
4. **Use the upcoming National Level Exercise 2020 to pilot the CICC model**

See 2019 report pages: 8 – 9

Closing Remarks

NIAC The President's National Infrastructure Advisory Council