National Infrastructure Advisory Council (NIAC)

Executive Order-Presidential Policy Directive Working Group (EO-PPD WG)

July 17, 2013

David E. Kepler
Executive Vice President/ Chief Sustainability Officer, Chief Information Officer
The Dow Chemical Company
Co-Chair

Philip Heasley
President and CEO
ACI Worldwide
Co-Chair

Agenda

- Framing Questions for Member Perspectives on Incentives
- Member Perspectives on Incentives
- Additional Perspectives Generated from Comments & Discussion
- Framing Questions for Member Perspectives on NIPP Re-write
- Member Perspectives on NIPP Re-write
- Appendix

Framing Questions

For Member Perspectives on Incentives

Framing Questions for Member Consideration

- What incentives are most likely to be adopted voluntarily by owners and operators?
- What incentives are least likely to be adopted voluntarily by owners and operators?
- Executive level engagement with the Federal government helps Executives create priorities, allocate resources, and hold individuals accountable for private sector actions. What steps can be taken to ensure Executives are engaged and driving voluntary incentive adoption?

Framing Questions for Member Consideration

- Executives are cognizant of their fiduciary responsibilities to shareholders. How can the Federal government best reduce risk and uncertainty for Executives and encourage voluntary incentive adoption?

- How can incentives best be paired with tools, technology, assets, and processes the government has, in order to encourage voluntary adoption?

- How can Executive Summaries on incentive implementation be precisely and concisely written for Executives with little prior knowledge or experience in critical infrastructure security and resilience in order to communicate what happens, how things work, and how their risk and uncertainty are reduced?

Framing Questions for Member Consideration

- How can the Federal government make all incentives voluntary while balancing regulation and oversight to facilitate a networked-coordination environment?
- How can incentives best target lifeline sectors most critical in an actual emergency?
- How can incentives best be prioritized to coordinate with infrastructures dependent on lifeline sectors that currently lack the resources, strength, or internal capabilities to bring themselves up to the level needed the case of an actual emergency?

Framing Questions for Member Consideration

- What steps should be taken to ensure that all NIAC members are fully aware of the alignment and structure of all 16 sectors in order to prioritize incentives and their voluntary adoption?
- To what extent should time limits and sunset clauses be incorporated to promote voluntary adoption?
- Are there additional incentive categories that should be considered in addition to the 14 proposed?
- Should any of the 14 proposed incentive categories be broken down further?
- Is their relevant research, literature, or Member experience that the Working Group should consider in either cyber or non-cyber contexts?

Member Perspectives

On Incentives

Grants are an effective means for encouraging adoption of a cybersecurity framework.

- Direct Federal funding for investment in the framework would be beneficial.
- It is important to clearly articulate any contingencies associated with the grants.
- Funding results should be outcome-based, and penalties should not exceed the value of the grant.
- Grants should be focused on creating capability that can benefit an entire industry sector, and not one company.
  - i.e. industry training programs, information sharing capability, research consortium for sector specific technologies, etc.

Liability caps are more effective than liability reductions.

- Security is not improved by simply transferring risk to insurance companies. A more effective strategy for encouraging participation would be to cap the liability associated with compliance with the cybersecurity framework.
- Not capping liability may create an environment in which insurance underwriters dictate security policy.
- Companies acting in good faith should not see additional risk in adoption of the framework.
- A policy similar to the SAFETY Act, which provides liability protection to encourage adoption of the “Cybersecurity Framework” or similar industry standard, should be considered as an option.

The Federal Government should require cybersecurity framework compliance on its suppliers, related to critical infrastructure.

- Government procurement power has numerous indirect benefits for the private sector. It incentivizes suppliers to enhance the security of their products and services — which are often the same products and services used in private critical infrastructure.
- The Government needs to include hardware and software suppliers in any scope of procurement policy. Reducing the risk associated with hardware and software systems allows owners and operators to redirect their attention to other critical security concerns.
- Many risks that CIKR owners/operators face are a direct result of vulnerabilities within purchased IT hardware and software.

Evaluation and leveraging of existing regulations

- Leveraging of compliance with existing laws into the framework is more effective than introducing new rules that may create conflict.
- Many cybersecurity policy and practices are already regulated.
- Layering additional policies and regulations on top of current regulations will create larger compliance models reducing flexibility, increase costs, and reduce effectiveness.

Additional Perspectives

Drawn from Member Comments
& Discussion

A robust, dynamic risk identification process

- Compliance with the cybersecurity framework compliance needs to be focused on the major risks in critical infrastructure.
- Greater credibility will be granted to a program that allows an owner/operator to focus adoption on the major risk areas. It will emphasize protection of vital assets, as well as reducing cost to both industry and the Federal Government.
- Rate recovery for price regulated industry is an effective incentive; however, keeping the focus on high risks lowers downstream consumer impact.

Ensuring the availability of qualified, vetted security professionals

- New areas of compliance require additional professionals to ensure compliance, and qualified personnel can be challenging to find.
- Federal assistance with background checks, and leveraging of existing programs could establish a greater reserve of qualified professionals.
- Further information:
  - NIAC 2006 Report on Workforce Preparation, Education and Research
  - NIAC 2008 Report on “The Insider Threat to Critical Infrastructures”

Anti-trust protection

- The effectiveness of the Executive Order and subsequent PPD relies heavily on the sharing of threat information between the public and private sectors, but also will require sharing amongst private sector companies. Currently this sharing is discouraged due to the concern of violating, or the appearance of violating, of Anti-Trust regulations. Government must provide Limited Anti-Trust vehicles that provide protections for companies that discuss and share cyber threat information.
- The NIAC previously noted the value of limited antitrust protections in its 2009 report, titled “Critical Infrastructure Resilience,” in relation to the Protected Critical Infrastructure Information (PCII) program. In that report, it was noted that the United Kingdom has enhanced risk information sharing among competitors by scrubbing the source of the information, and focusing only on mitigation methods, and that a similar set of rules could dispel fears of using such information against the entity providing it.

Framing Questions

For Member Perspectives on National Infrastructure Protection Plan Re-write

Framing Questions for Member Consideration

- How does the Federal government write a short and clear revised plan that is flexible adaptable, and readable to owners and operators outside of the Beltway?
- What has to be in the plan for it to be seen as useful and applicable to owners and operators?
- How do we incorporate the concepts of how the critical infrastructure mission can operate in a “networked-coordination” environment; but provide enough structure and order that those who are going to be implementing the NIPP can build their own plans, processes, etc.in a measurable way from a national perspective?

Framing Questions for Member Consideration

- How can the plan focus on critical functions and services (such as the lifeline infrastructures and dependencies by the other sectors) while maintaining appropriate and relevant risk based momentum in the other sectors?

- How can the plan incorporate appropriate support for the 4.8 Million O/O community (baseline) so that they also can benefit from the national programs, capabilities, and lessons learned; that they know what to do and where to go for infrastructure security and resilience information and advice/guidance (given continuous restrained Federal resources)?

Member Perspectives

On National Infrastructure Protection Plan Re-Write

Executive-level engagement is vital in any effort to encourage private sector use of the NIPP, and should be embraced in every public-private partnership activity.

- Executive-level private sector officials set priorities, direct resources, and can hold others accountable within the corporation. Because of this, the success of any partnership with owners and operators is contingent upon successful engagement with those who have the most ability to direct a company toward a more secure and resilient posture — CEOs and executives with board member oversight.
- The revised NIPP should include a summary for these officials to improve the understanding of the critical infrastructure security and resilience (CISR) mission. The Federal Government should seek input and help from the private sector to develop a communication plan targeted at Senior Business Leaders that may include meetings with senior executives, CEO forums, and executive summaries to further explain the relevance of the NIPP. This should include sector specific messaging.
- In addition, an advisory panel — with the ability to guide and mold the development of a flexible, adaptable, outcome based plan — should be considered as a means to enhance the value of the document.

To make the plan useful and valuable to the private sector, clear, concise communication incentivizing the public-private partnership value proposition is needed.

- There are numerous tools, technologies, and programs created by the Federal Government and Industry that can assist in risk assessments and risk management. A simple description of how these programs can reduce risk, along with an explanation of the participation process, would better inform senior-level private sector stakeholders on the value of the NIPP framework. For example, the Chemical sector, DHS developed the CFATS program that helps assessing risk and security practices. The National Institute of Standards and technology (NIST) also provides guidance that can be leveraged. Established Industry standards like ISO 27001 and ISA /ISEC 62443 series for Industrial Automation can be used as well during NIPP revision.
- Examples of successful public-private partnership efforts would provide real-life demonstrations of the value drawn from the NIPP, and how a company can collaborate in the networked environment.

The four "lifeline sectors" – water, electricity, communications and transportation – should be the focus of prioritized efforts to enhance security and resilience, with a recognition of the importance of information technology to those sectors.

- Rather than attempting to dedicate equal attention to all 16 critical infrastructure sectors, the effect each sector has on the well-being of the Nation should be taken into consideration. "Lifeline Sectors" — Water, Electricity, Communications, and Transportation — are regarded as central to the Nation; as a result, those sectors should receive the largest share of immediate attention in the effort to increase security and resilience. Limited Federal resources should not be diluted by applying equal immediate effort to each sector; instead, a tiered system should be established to guide prioritization. Of the remaining critical infrastructure sectors, importance will vary among regions but the financial sector stands out as being important to national economic activity.
- Sectors which supply critical IT hardware and software to CIKR sectors also need appropriate attention. All CIKR sectors rely heavily on IT backbone products such as operating systems, network hardware, process control systems, etc. Secure backbone products create resiliency throughout the entire supply chain.

Development of the implementation plan should be a collaborative effort between the Federal Government and owners and operators.

- Plans that are considered, developed, and deployed solely by Federal agencies often produce actions only for the Federal Government itself. A high-level public-private partnership planning group — featuring industry executives and practitioners, as well as senior-level Federal officials — could produce a more effective plan by addressing the issues facing all stakeholders in the partnership.

It is important to have a voluntary structure for private sector participants, and that regulators are guided in the navigation of the public-private partnership.

- The Federal Government should be careful to ensure that regulatory bodies do not attempt to impose their will onto the partnership. Punitive oversight measures would only be counterproductive to efforts to enhance the public-private partnership.
- A commitment to educate regulators is also needed from the Federal Government on evaluation and consideration of those owners and operators collaborating on the CISR mission and partnership.
- The Federal Government should seek the support from the private sector to educate its regulators and Industry on Cyber security practices being implemented in the Industry. Private Sector is willing to help in the development and education of the regulators.
- It is also recommended that those entities in the partnership are granted some protections from regulative bodies as they work to improve security and resilience.

Providing services which can be leveraged by the broader owner/operator community

- One of the key challenges that NIPP revision will have is to address is incorporating appropriate support for the broader 4.8 Million O/O community. To address it, The Federal Government can influence the private sector IT companies to play a bigger role in helping to uplift the security posture of the 4.8 million O/O community. While standards and information sharing will play a big role in this endeavor, Operators are often overwhelmed and under-informed when choosing the right security technology and identify the "threat indicators". Creating a common national cyber threat database which is populated by both public and private entities and available by subscription to all owner / operators would eliminate some of the barriers in picking the technology and security practices needed by a company to effectively implement a cyber security framework.
- This is an area where grant incentives may be considered.

Appendix

Working Group Members

WG Member	Sector Experience
David E. Kepler, *Executive Vice President/ Chief Sustainability Officer, Chief Information Officer, The Dow Chemical Company*, Co-Chair	Chemical
Philip Heasley, *President and CEO, ACI Worldwide*, Co-Chair	Telecommunications
Glenn S. Gerstell, *Managing Partner, Milbank, Tweed, Hadley, & McCloy LLP*	Water, Telecommunications
Michael J. Wallace, *Former Vice Chairman and COO, Constellation Energy*	Electricity, Nuclear