National Infrastructure Advisory Council (NIAC)

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

November 21, 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

- Study Overview
- General Observations
- Findings
- Recommendations
- Next Steps

Study Overview

Working Group Members

WG Member	Sector Experience
David Kepler, *Chief Sustainability Officer, Chief Information Officer, The Dow Chemical Co.* (Co-Chair)	Chemical
Philip Heasley, *President and CEO, ACI Worldwide* (Co-Chair)	Financial Services
Constance H. Lau, *President and Chief Executive Officer, Hawaiian Electric Industries, Inc. (HEI)*	Electricity, Financial Services
Glenn S. Gerstell, *Managing Partner, Milbank, Tweed, Hadley, & McCloy LLP*	Water, Telecommunications
Michael J. Wallace, *Senior Advisor and Director, Nuclear Energy Program, Center for Strategic and International Studies, Former Vice Chairman and COO, Constellation Energy*	Electricity, Nuclear

Background

Background

Incentives for Adopting the Cybersecurity Framework

- Successful implementation of the voluntary cybersecurity framework is reliant on widespread buy-in from private sector owners and operators, and incentives are a key component of generating interest and participation.
- The Administration offered several potential incentives that could assist in encouraging adoption of the voluntary cybersecurity framework.
  - The NIAC was asked to review these options, determine the relative value and the likelihood of adoption of each incentive, and to suggest any additional incentives that would encourage greater participation.

Background, continued

Information Sharing

- The NIAC was asked to consider information sharing, and the successes and challenges of the current public-private information sharing environment.
- Issues under consideration included obstacles to effective information sharing; incentives to encourage increased sharing; effective mechanisms; the differences between physical and cyber information sharing; principles to encourage voluntary participation; the core principles for cyber information sharing; and the appropriate metrics for the sharing of cyber threat information.

Background, continued

Cybersecurity Framework

- In reviewing elements of the proposed cybersecurity framework, the NIAC was asked to determine the aspects of the framework most likely to benefit private sector owners and operators.
- Issues under consideration included the elements that would facilitate widest adoption by owners and operators; efficient and effective processes to facilitate adoption; how to best measure participation in and the value of the framework; obstacles preventing adoption, particularly for non-Fortune 500 companies; which audiences to target; and any issues that require the alignment of Federal agencies with other levels of government.

Background, continued

NIPP revision

- As part of PPD-21, DHS is revising and updating the National Infrastructure Protection Plan.
- The NIAC was asked to review drafts of the revised documents, and offer comments on concepts including how the Federal Government can provide a clear, concise, flexible, and adaptable plan; what should be included to make the plan valuable to owners and operators; how to include a focus on critical functions and services, while maintaining appropriate and relevant risk-based momentum; and determining the forms of support that will allow the wider owner-operator community to benefit from the plan.

Findings

Key Findings – Cybersecurity Framework Adoption

1. The key factor to encourage adoption by the private sector of the Cybersecurity Framework is **creating confidence that it is effective in securing the nation from cybersecurity threats.**
2. The incentives most likely to encourage confidence and participation of critical infrastructure owners and operators are **an effective framework, good-faith protection of shared information, streamlining of regulations, and outcome-based metrics.**
3. Focus on Purpose - **Implementation will be better served by focusing on the Critical Purpose and related outcomes**, such as goals and metrics, that allow the private sector to continue to implement effective cybersecurity systems, while expanding the public-private partnership.

Key Findings – Information Sharing

4. **Creation of a Safe Harbor - with limited antitrust protection —ensures information is used for intended purposes only, and offers protection from liability** when acting in good faith will encourage participation in the Information Sharing program.
5. Information - **The opportunity to receive timely, actionable information is the most significant incentive** in encouraging companies to participate in the information sharing program.
6. Classification of Information - **Over-classification of information is a significant barrier to effective information sharing programs.**

Key Findings – Information Sharing, continued

7. Intended Use - The private sector is concerned that **the sharing of some forms of information could lead to governmental inquiries and regulation beyond the original purpose** for which the information was offered.
8. Information for Critical Purpose - As stated in the National Infrastructure Protection Plan, **information sharing is a means to an end, not an end itself.**

Key Findings – Cybersecurity Framework

9. **Metrics and milestones that measure outcomes will be key to the success of the cybersecurity framework**.
10. Evergreen Process - **An ongoing effort will be required in order to gain the most value from the cybersecurity framework**.

Key Findings – NIPP Revision

11. Collaboration - **The emphasis on promoting collaboration between governments and the private sector in development of the NIPP is particularly likely to increase the plan's chances of success**.
12. Risk Prioritization - **A risk management methodology is the right approach for determining the capabilities needed** to enhance infrastructure security and resilience.
13. Centralized Ownership - **Housing of the Security Framework within an educational institution can help further develop the framework** and promote the benefits of private sector adoption.

Recommendations

Recommendations – Cybersecurity Framework Adoption

1. Limit liability on damages resulting from cybersecurity events.
   - Liability limits are an effective incentive to drive adoption of the cybersecurity framework by industry.
   - However, the Council cautions against the creation of an environment where insurance underwriters are dictating security policies.
   - Transferring risk to insurance companies does little to bolster security.

Recommendations – Cybersecurity Framework Adoption

2. Use the Government's procurement power to encourage information technology suppliers to develop cybersecurity framework-compliant hardware and software.
   - Government procurement practices have numerous indirect benefits for the larger critical infrastructure community.
   - It incentivizes suppliers to enhance the security of their products and services, which are often the same products and services used throughout the critical infrastructure security and resilience (CISR) community.
   - Improvements to those systems and reducing the risk associated with hardware and software gaps also allow owners and operators to redirect their attention to other critical security concerns.

Recommendations – Cybersecurity Framework Adoption

3. The Government should ensure 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.

Recommendations – Cybersecurity Framework Adoption

4. Grants, if used, should be focused on capacity building.
   - Direct Federal funding for investment should encourage adoption of the framework, through training, implementation, and more robust IT products, especially for small- to medium-sized operators.
   - Any contingencies placed on grants must be outcome-based and clearly articulated.
   - Penalties for low success should not exceed the value of the grant.

Recommendations – Cybersecurity Framework Adoption

5. "Metrics for Measuring of Efficacy of Critical Infrastructure Centric Cybersecurity Information Sharing Efforts," by Fleming/Goldstein 2012, should be leveraged in creating outcome metrics that can be used to measure the success of the EO and PPD implementation, including metrics such as indicators shared, attacks prevented, attackers caught, and risk mitigated.
6. The cybersecurity framework should be housed at a university, with base funding coming from critical infrastructure companies.

Recommendations – Engagement of small- and mid-sized owner/operators

7. The Federal Government should put forward additional effort to assist small- to mid-sized owners and operators in meeting the critical purpose outlined in EO 13636, in order to ensure reliable functioning of the Nation's critical infrastructure in the face of cyber threats, including:
   - Government-funded programs at universities to develop training to understand and best leverage the cybersecurity framework.
   - Government encouragement of IT providers and suppliers to create products that have security as a primary design criteria.

Recommendations – Engagement of small- and mid-sized owner/operators

- Government-developed training to assist small- and medium-sized owners and operators who lack resources or expertise.
- Centralized ownership of the Security Framework within an educational institution to further develop the framework and promote the benefits of private sector adoption.
  - Successful examples of this type of development within the education sector can be found within Carnegie Mellon's Software Engineering Institute - Community Emergency Response Team (CERT) program.

Recommendations – Information Sharing

8. The Federal Government should adopt a policy that specifically addresses concerns that information sharing could lead to governmental inquiries and regulation beyond the original purpose for which the information was offered.

Recommendations – NIPP Revision

- Security should be designed to be built in to systems, rather than layered on top of systems.
- The Government should leverage its purchasing power to incentivize enhanced security and resilience in core cybersecurity systems and programs (Information Technology, Industrial Automation, and Telecommunications sectors).
- The Framework should include standards that address the risk management of Industrial Automation systems, which have unique control characteristics apart from general cybersecurity. Industrial Automation may warrant its own sector category.

Recommendations – NIPP Revision, continued

- The Government should develop policies and apply resources to pursue and discourage global cyber criminals from attacking critical infrastructure facilities.
- The revised NIPP should include a summary specifically written for executives, in order to improve the understanding of the CISR mission.
- The Government should convene a public-private advisory panel under CIPAC to ensure that the needs of the private sector are addressed in the implementation of the revised NIPP.

Questions?