National Infrastructure Advisory Council (NIAC)

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

September 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 on the Cybersecurity Framework
- Positive Working Group Member Observations on the Cybersecurity Framework
- Working Group Member Recommendations on Areas For Future Improvement Concerning the Cybersecurity Framework
- Working Group Recommendations for Maximum Adoption of the Cybersecurity Framework
- Appendix

Framing Questions

On the Cybersecurity Framework

Framing Questions

- What necessary elements must be in the Framework in order to facilitate broadest adoption by owners and operators?
- What might be the most efficient and effective processes facilitating adoption, and what can the government do to facilitate?
- What is the best way for the Government to measure usefulness and adoption of the Framework?

Framing Questions Continued

- What are the obstacles preventing adoption, particularly for those organizations outside the Fortune 1000?
- What do you recommend as the target audience(s) and the message to facilitate adoption?
- What issues may exist requiring alignment across Federal agencies, regulatory and non-regulatory, and with other levels of government? What would you recommend addressing these issues?

Positive Observations

From the Working Group on the Cybersecurity Framework

Positive Observations

- Care has been taken throughout the development process to stress that use of the Framework is voluntary.

- The Function, Category and Subcategory hierarchy in the Framework core are very similar to those hierarchies included in Quality Management Systems plans.
  - This allows for flexibility in application.
  - The concept of "tiers" is similar to levels typically seen in IT Industry capability maturity models.

Positive Observations Continued

- There is specific and actionable guidance on how to apply the Framework (Section 2.4), including some practical examples.
- Partnership between government and the private sector is emphasized, not only in the development of the Framework, but in its continued application.
- A risk-based approach is used, acknowledging that there are differences by industry or sector; cyber risk management should be integrated with existing processes, and is not something separate.

Working Group Recommendations

On Areas For Continued Improvement

Working Group Recommendations on Areas For Continued Improvement

- A focus on both process and outcome-based metrics as a means of assessing effectiveness in applying the Framework.
  - See "Metrics for Measuring the Efficacy of Critical Infrastructure Cybersecurity Information Sharing Efforts," by Flemming/Goldstein (2012)

Working Group Recommendations on Areas For Continued Improvement

- More specifics are needed regarding who will have ownership of and responsibility for the continued development of this Framework once released.
  - We agree with the stated goal for this to be in the private sector.
  - We would recommend housing it at a university, with base funding coming from critical infrastructure companies.

- The Framework should include sections on information sharing and benchmarking to ensure that companies establish processes to gather cyber intelligence and to assess cyber programs versus industry trends and practices.

Working Group Recommendations on Areas For Continued Improvement

- Details should be developed about the mechanisms that will be used to improve and develop this model, and to coordinate its application for the purpose of sharing of experiences.

- Additional basis for, and emphasis on, security standards for IT products is required (i.e., "Secure by Design" concept).
  - This is a critical foundational element of the framework. For industrial control systems, the ISA/IEC 62443 series addresses this specifically.

Working Group Recommendations on Areas For Continued Improvement

- Given the focus on lifeline sectors (Energy, Water, Transportation and Telecommunications) and their interdependencies, more emphasis on Process Control Systems and the specific or unique characteristics or constraints is required.
  - (Private sector is continuing to address this through collaboration between ISA, the Automation Federation and the developers of the Framework.)
  - For example, the precedence of Confidentiality over Integrity and Availability that is typical for information systems changes to a preference for Availability and Integrity over Confidentiality for industrial systems design.

Working Group Recommendations

For Maximum Adoption of the Cybersecurity Framework

Critical Purpose: National and Economic Security from Cyber Threats

- This Critical Purpose is clearly outlined by the President in Executive Order 13636 (EO):
  - "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved Cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."

Key Principles

- Focusing first on securing the lifeline sectors (Energy, Water, Transportation, and Telecommunications) and their interdependencies.

- Engaging participation of the IT Sector in the recognition that improving quality and security of IT products and services are required to protect the cyber backbone of the lifeline sectors.
  - In addition, government agencies and the financial sector and their networks are a foundation to these lifeline sectors, and will need a high-priority focus.

Key Principles Continued

- Using an outcome-based process in identifying significant risks and their mitigations, including response preparedness.

- Sharing of relevant and actionable information between the government, private sector participants and their peers, with adequate protection to ensure the information is used for the Critical Purpose.

Key Principles Continued

- Leveraging and aligning existing standards, management systems and regulations that are demonstrated to work towards achieving the Critical Purpose.

- Pursuing and prosecuting those participating in cyber criminal and espionage acts.

Primary Incentives

- Confidence that the framework will be effective in improving security posture, in a cost-effective manner:
  - There are clear outcome-focused objectives and goals in securing CIKRs
  - There is transparency and focus on the high-priority threats.
  - National Cybersecurity program and framework have clear and effective implementation plans

Primary Incentives Continued

- Information that is shared in addressing cybersecurity is used for security purposes only.
  - These include limited protection for liability, antitrust, and limit to government access for other use when a company acts in good faith.
- Streamline and removal of duplication within existing regulations.
  - Develop a cybersecurity risk framework that leverages or gives credit for the compliance with existing regulations (SoX, HIPAA, CFATS, etc.) and avoids duplication of effort, including elimination of compliance with multiple standards.
- There are clear, outcome-based metrics (see appendix), with commitments to improve these requirements.

Conclusion

- Having national unity of effort to strengthen and maintain a secure, functioning, and resilient infrastructure requires broad participation, collaboration, and trust.
  - The probability of success will be improved by incorporating the key principles and outcome-based deliverables stated above in all aspects of EO 13636 & PPD 21.
- The NIAC working group will re-frame its previous responses in the context of these principles, and will provide future responses in this context as well.
- It is recommended that the President factor these principles into the development of the Cybersecurity Framework.

Appendix

Table ES1. Metrics for Measuring the Performance of Critical–Infrastructure–Centric Cybersecurity Information Sharing

Inputs	Processes	Outputs	Outcomes
Shared information comprises both data and meaning: ▪ % of participating entities reporting that shared information received in a given time period contains both data and meaning ▪ % of submitted information and analytic products (based upon a random sample) that contain both data and meaning **Shared information is relevant:** ▪ % of participating entities reporting that the shared information they receive in a given time period informs decisions that reduce cyber risks to critical infrastructure ▪ % of participating entities reporting that the shared information they receive in a given time period contains new data, new meaning, or both ▪ % of *specific* information submissions or analytic products released in a given time period that inform decisions, and contain new data, new meaning, or both ▪ Number of instances in a given time period that *specific* submissions or products that were not yet known about led to the discovery of a previously unknown cyber incident, once deployed	**The goal is specified:** ▪ % of participating entities reporting that the goal has been developed, issued, and disseminated by a coordinating body **The goal is agreed upon:** ▪ % of participating entities providing express or implied concurrence with goal **Participating entities are appropriate:** ▪ % of participating entities who meet specified criteria ▪ % of participating entities who report that they can generate, analyze, or use information to achieve the goal **Entities are participating:** ▪ % of entities logging on to the information sharing website at least once in a given time period ▪ % of entities sending information to the website at least once in a given time period ▪ % of entities receiving information from the website at least once in a given time period ▪ % of entities participating in scheduled collaborative exchanges in a given time period ▪ % of entities with at least one person on the NCCIC floor at least once in a given time period ▪ % of entities who report independent collaboration with other entities in a given time period ▪ % of entities responding to RFIs in a given time period	**Information is used for tactical and strategic purposes:** ▪ % of participating entities reporting use of shared information to improve or implement security controls in a given time period (tactical use) ▪ % of participating entities reporting use of shared information to inform resource allocation decisions in a given time period (strategic use) ▪ % of received (i.e., accessed) information used to improve or implement security controls in a given time period (tactical use) ▪ % of received (i.e., accessed) information used to inform resource allocation decisions (strategic use)	**Goal is achieved** (all in a given time period): ▪ Number of incidents causing unavailability of critical services and estimated associated costs of damage ▪ Number of incidents causing the loss of critical data and estimated costs of damage ▪ Number of detected incidents, both prevented and successful, and estimated costs of damage ▪ Unplanned downtime ▪ Mean time to incident detection ▪ Mean time to incident remediation ▪ Mean time to incident recovery ▪ Mean time between failures

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, *Senior Advisor, Center for Strategic and International Studies (CSIS), Director, Nuclear Energy Program*	Electricity, Nuclear
Constance H. Lau, *President and CEO, Hawaiian Electric Industries, Inc.*	Electricity