National Infrastructure Advisory Council (NIAC)

Executive Order 13636 and PPD-21 Working Group

Recommendations for Maximum Engagement, Including the Cybersecurity Framework, in Reducing Cyber Risks to Critical Infrastructure

The National Infrastructure Advisory Council (NIAC) working group has had the opportunity to review a series of questions covering the material being produced by the Integrated Task Force (ITF). All of this work, including the Cybersecurity Framework, can be best aligned by ensuring two fundamental questions are addressed. 1) What is the Critical Purpose and how will achieving this purpose be measured?; and 2) What will incentivize the private and public sector to collaborate effectively to address the Critical Purpose?

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."

This NIAC working group agrees with the President's sense of urgency. The development and implementation of Executive Order 13636, Presidential Policy Directive (PPD) 21; including the framework, their structure, processes and participation; must be based on this critical outcome. Metrics and Milestones to measure the outcomes will be key to the framework's success.

September 4, 2013

The key principles must include;

1. Focusing first on securing the lifeline sectors (Energy, Water, Transportation, and Telecommunications) and their interdependencies.
2. 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.
3. Using an outcome-based process in identifying significant risks and their mitigations, including response preparedness.
4. 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.
5. Leveraging and aligning existing standards, management systems and regulations that are demonstrated to work towards achieving the Critical Purpose.
6. Pursuing and prosecuting those participating in cyber criminal and espionage acts.

The Primary adoption of a program is the belief that the program is effective with a clear purpose.

These primary incentives, more than all others, will incentivize Critical Infrastructure and Key Resources (CIKR) executives to participation:

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

2. 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.
3. 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.
4. There are clear outcome based metrics (see note 1), with commitments to improve these requirements.

Implementation will be better served by focusing on the Critical Purpose and related outcomes (goals and metrics), which allows the private sector to continue to implement effective cybersecurity systems, while expanding the public-private collaboration. There are successful examples in the industry of effective systems, such as the Occupational Safety and Health Administration (OSHA) Voluntary Protection Program (VPP), or the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. Similar processes could be enacted for cybersecurity, which would provide proactive risk management reviews of participating CIKR organizations that would benefit from Federal Government cybersecurity expertise. Those organizations that are certified as “effectively managing risks” would be given incentives in terms of reducing overlapping regulations and inspections or offering liability protections.

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 factors these principles into the development of the Cybersecurity Framework.

Notes :

(1) It is recommended that the document “Metrics for Measuring the Efficacy of Critical Infrastructure Centric Cybersecurity Information Sharing Efforts,” by Fleming/Goldstein (2012), be leveraged in creating outcome metrics that can be used to measure the success of the EO and PPD implementation. Such metrics might include indicators shared, attacks prevented, attackers caught, risks mitigated, etc.