National Infrastructure Advisory Council (NIAC)

Executive Order 13636 and PPD-21 Working Group

Recommendations on Cybersecurity Information Sharing

August 8, 2013

At a high level, the EO-PPD information sharing framework is aligned with the private sector's need for sharing timely and actionable information. This program as being developed can benefit all critical infrastructure sectors.

A significant challenge is to share information in a timely, specific and actionable way between the Government and private sector. Creation of a "safe harbor", a recognition that information will only be used for intended purposes combined with limited anti-trust and privacy regulation protection, when acting in good faith, will encourage greater private sector participation in the Information Sharing program.

1. **Incentives**:
   The opportunity to receive timely and actionable information, by itself, is a significant incentive for companies to opt into the information sharing program. Additional incentives could include technical guidelines, support and sharing of cyber security practices between DHS/NSA and the private sector.
2. **Effective mechanisms**:
   The private sector needs easy access to indicators via a portal similar to those used by HSIN and US-CERT. Information must be in a format and specificity that can be used by each company to search their own security logs (i.e. IP addresses, domains, malware hashes, etc.).
   Sharing specific vulnerabilities, threats, methods and motivations of attackers will also help private sectors make more accurate and effective use of resources to improve cybersecurity postures.
   All current Federal mechanisms for Information Sharing (one-on-one, US-CERT, intelligence briefings,…) should be reviewed with the goal of simplifying processes, eliminate redundancy , improve coordination

among different Federal agencies and ensure consistency of information delivered as suggested by NIAC in 2012.

DHS should collaborate with the private sector on information sharing work process definition, to ensure that procedures are effective and efficient for exchanging information between the owners and operators and government at all levels.

3. **Classification of information in the management of Cybersecurity**:
   Another significant barrier to an effective information sharing program is the structure in how information is classified. Information needs to be more finely divided, so that as much of what is shared as possible can be declassified. That will allow more information to be disseminated among the private sector to resources that can take specific actions. Although DHS plans to expedite clearances, there needs to be more clarity on how classified information can be used within a company whose monitoring systems will not be certified for classified information. If action is to be taken, information needs to be declassified for deeper and broader communication within a company or industry. Execution of cyber security does not just fall within the CISO or CIO. Unlike some information that could be actionable despite being highly compartmentalized, because of the use and implementation of Information Technology systems and controls across entire facilities and organizations, there is a need for cybersecurity information to be disseminated more broadly. This direction has been provided for in the new Executive Order.
4. **Principles to encourage information sharing**:
   Recognizing that the concerns of the private sector in sharing information may inhibit the desired level of this sharing, the Federal government should adopt a policy that specifically addresses concerns that information sharing could lead to governmental inquiries and regulation beyond the original particular purpose for which information may have been offered. DHS PCII (Protect Critical Infrastructure Information) is a good example of a program that can be leveraged in other sectors to address this concern. To allay such concerns, and in

appreciation of the greater benefits that may arise from encouraged information sharing by the private sector to the public authorities, the Federal government could, for example, provide mechanisms to assure that information will remain confidential and not disseminated within the government except where there are legitimate and compelling reasons to do so. To further illustrate, such mechanisms might range from the designation of particular means and channels of communication to assure confidentiality, to the creation of "safe harbors" whereby private sector entities could have limited anti-trust protection, the ability to divulge information free of civil or criminal liability under privacy protection laws, and to the establishment of exceptions for disclosure regarding cyber incidents by SEC public reporting companies under limited conditions.

5. **Metrics:**

   As stated in the National Infrastructure Protection Plan, information sharing is a means to an end, not an end itself. An information sharing effort should recognize, understand, and concur with a common goal. The Homeland Security Studies and Analysis Institute (HSSAI), a non-profit federally funded research and development center operated by Analytic Services Inc. on behalf of the DHS has created document entitled "Metrics for Measuring the Efficacy of Critical Infrastructure-Centric Cybersecurity Information Sharing Efforts. This document details options for metrics which include the attributes of effective information sharing (i.e. relevance, timeliness, accuracy, etc.) and the outcome based goal of information sharing which is primarily 'no loss of control'. We recommend that, if the Integrated Task Force is not leveraging this document, that it serve as the framework for the development of the metrics.