Working Group Recommendations
National Infrastructure Protection Plan Feedback

National Infrastructure Protection Plan (NIPP)

Several themes were noted in response to questions posed regarding the revision of the NIPP. These overarching themes are listed in bold below:

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.