National Infrastructure Advisory Council (NIAC)

Executive Order 13636 and PPD-21 Working Group

Recommendations on NIST Cybersecurity Framework

September 4, 2013

The latest draft of the framework presents a coherent approach to crafting an effective cyber security program based on established standards and practices.

Positive observations include:

- 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.
- 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.

The Framework description also includes several areas for future work, a recognition that this will be an ongoing effort. Specific areas for further consideration or improvement should include:

- 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).

- 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.
  - 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.
  - 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. The 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.