

April 8, 2013

Response to NIST RFI

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Section 1

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?
 - Legacy infrastructure and devices that were implemented in the past without cybersecurity in mind.
 - Lack of stringent cybersecurity measures required for vendors, solution providers, and their products.
 - Lack of education and proper cybersecurity training across the employee base within organizations.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
 - Integration of multiple standards and controls from a variety of specific industry segments will be a challenge to achieving an effective cybersecurity framework.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?
 - The electric industry critical assets are necessary for the remaining critical infrastructures to perform properly. It is imperative that the critical assets and systems remain available at all times.

12. What role(s) do or should national/international standards and organizations that develop national/ international standards play in critical infrastructure cybersecurity conformity assessment?
 - National/International standards and organizations should play a pivotal role in providing the foundation for a cybersecurity conformity assessment. A single experienced body that can provide coordination and guide the effort is important to the effort. That body should work with both public and private organizations to lead, gather data, manage communication, and consolidate the information and provide a successful assessment and framework.

Section 2

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?
 - The Department of Homeland Security (DHS) National Infrastructure Protection Plan (NIPP) is a proven and effective approach for providing a unifying guideline that integrates a variety of cybersecurity efforts that can be utilized to enhance the framework.
 - The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) is a recent proven risk maturity model that would be effective for enhancing the framework.
2. Which of these approaches apply across sectors?
 - The NIPP would apply across all sixteen of the critical infrastructure sectors.
3. Which organizations use these approaches?
 - Each of the infrastructure sectors could utilize the NIPP approach.
4. What, if any, are the limitations of using such approaches?
 - Like all standards, guidelines, and plans, there is no “one size fits all” approach across multiple sectors and organizations. Therefore additional analysis and coordination should be performed to ensure the requirements are applicable.
5. What, if any, modifications could make these approaches more useful?
 - The ES-C2M2 would have to be modified to be applicable to the other sectors. It is Energy sector focused but does contain some valuable risk measurement tools.
6. How do these approaches take into account sector-specific needs?
 - NIPP as well as ISO-27001, and existing NIST standards are sector and technology agnostic. Each organization should work within its sector and determine what requirements and guidelines are relevant to fit its systems and environments.
7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?
 - Most of the sectors already have sector-specific standards in place. The NERC standards require mandatory compliance from organizations within the electric industry.

Section 3

Specific Industry Practices

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?
 - Identification and authorization of users accessing systems
 - Asset identification and management
 - Monitoring and incident detection tools and capabilities
 - Use of encryption and key management.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?
 - The requiring of security practices and controls for vendors and their products.