April, 8, 2013

From: Frank Knickerbocker, ANSER, an Operating Unit of Analytic Services Incorporated

Subject: "Developing a Framework to Improve Critical Infrastructure Cybersecurity" NIST RFI of 2/26/2013 – Response to select questions

What follows are ANSER's responses to selected questions posed in Federal Register Notice, dated February 26, 2013, on the subject of *Developing a Framework to Improve Critical Infrastructure Cybersecurity* by the Department of Commerce/National Institute of Standards and Technology (NIST). We are a not-for-profit public research institute providing independent analysis and support to public agencies for more than 50 years. We have extensive experience helping Government clients at all levels conceive, design, implement, apply and continuously improve intellectual frameworks, technical and operational standards, and best practices in a wide variety of operational, management and technical domains.

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Like many organizations, ANSER faces the multi-tiered challenge of instituting and improving cybersecurity practices and capabilities. From our view in engagement with clients in the federal government sector, across multiple implementation disciplines, the greatest challenge is access to cybersecurity considerations within each implementation discipline, such as security and counterterrorism, chemical-biological defense, health protection, and nuclear weapons handling. Cybersecurity practices across this diversity of operational domains and associated critical infrastructure are challenged by limited access to operationally relevant cyber practices which have context within their associated risk probabilities and impacts.

No single repository of data on all of the laws, regulations, ordinances, memoranda of agreement, policies, directives, etc. detailing cybersecurity responsibilities and authorities can nor should be compiled. This challenge will be best addressed by a framework which operates in at least two tiers. The first tier, unifying principles and core practices, may be elaborated in the second tier within specific sectors and operational domains. Conceivably, these tiers can be extended to lower levels of specification.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Based on our experience within the public sector, the greatest challenges in developing a framework for cross-sectors include, but are not limited to:

- Diverse organizational cultures, roles, responsibilities and governing structures
- Disparate Business and IT systems and technology specific assessment of risks
- Lack of public engagement and inputs from public stakeholders
- Cybersecurity requirements introduced late in the developmental processes (acquisition, manufacturing, policy)
- The right level of oversight , correctly metered by relevant risk assessment methods and based on current cybersecurity standards, policy, and guidance
- Integration of Privacy and Confidentiality impacts into risk methodologies and reporting processes, especially respecting the differentiated roles of government and business

As a corporation that employs applied systems thinking, we view developing the cybersecurity framework as an effort in systems of systems engineering (SoSE). While all share many aspects of the cybersecurity challenge, the unique nature of each set of organizations (in the form of individual companies, temporary alliances, supply chains and extended enterprises, long-standing partnerships or even whole business sectors) inevitably demands expression in the conduct of their business. The framework must enable overall success without compromising individual freedom. This means that attempts to create a "one size fits all" approach will meet strenuous and active resistance, inevitably leading to failure. Our experience addressing similar challenges in other domains leads us to conclude that the goal should be a framework that is *both based on a common core of standards and extensible* by individual organizations and collections of organizations (ranging in size from teams to industries to sectors). Creating the core will likely require adopting a layered (or tiered) approach not unlike that used when designing computing architecture. Integration of capabilities across and communication of information among the layers will be key. Viewed in this light, the design of trusted, responsive governance and integration structures and processes will be the paramount challenge.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

Analytic Services Incorporated reports to the Defense Security Service for security compliance, including cybersecurity. This is a requirement of the predominant proportion of our business relationship with Federal, Department of Defense, clients. We note that as we initiate each client relationship, we must crosswalk all applicable regulations and policies for overlaps and gaps in policy and instruction. Alignment tools for these types of considerations would be a very welcome part of the framework.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Our corporation is dependent upon the telecommunications sector primarily, and the energy (electric) sector as most important. We would like to develop a deeper understanding of the interdependencies and how to identify the weakest cyber link in these sectors as well.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Critical infrastructure has sovereign national definition, but supranational impacts. It is very likely we will encounter international treaty relationships requiring and/or affecting definition of cybersecurity terms of reference among sovereigns as the linkages between cybersecurity to commerce and other international concerns becomes better defined.

National and international standards organizations should remain immersed within a free-flowing discourse identifying ideas, best practices and commonalities, with both limited and broad application. National and international organizations must span sectors between conformance entities (such as government) and entities which must conform (such as business). To most effectively preserve their relationship to the critical information sources among these entities, their role should be in identification and consensus elicitation for conformity assessment. Implementation and enforcement of conformity would remain with the entities so empowered.

Use of Frameworks, Standards, Guidelines, and Best Practices

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Sectors will generally vary in their nature regarding voluntary or compulsive framework effectiveness. We recommend an assessment of the comparative effectiveness of each type to the organizational context at hand. Each organization will perceive importance and impact of the sectors differently. The bottom line is “what is the value added” by adoption and implementation of the framework. Decision makers will require a mechanism by which they can assess value in terms of relevant goals. This assessment must be capable of discriminating the marginal value of investment for each sector (or sub-element, as applicable). Decision makers must also have access to pertinent and robust cost-benefit-risk analyses. These analyses would be linked to operational process analysis capabilities. Operational diversity in implementation of cybersecurity will persist; therefore, the framework for cybersecurity should reference standards and methods for operational process analysis and interrelationships.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The Framework development effort may benefit from an examination of the governance structure and processes used by the Office of the National Coordinator for Health Information

Technology (ONC), a staff division within the US Department of Health & Human Services (HHS). The position of National Coordinator was created in 2004, through an Executive Order, and legislatively mandated in the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009. The ONC is primarily focused on coordination of nationwide efforts to implement and use health information technology and the electronic exchange of health information. The ONC oversees the Nationwide Health Information Network. The ONC website is http://www.healthit.gov/

9. What other outreach efforts would be helpful?

We recommend one of the most important outreach efforts is to establish a support structure to promote, educate, train and mentor stakeholders on the use of the Framework. Having this structure will facilitate transition for organizations into the implementation of the Framework. An insufficiently robust support function may lead to inconsistencies in use that increase the risk of failure in either or both adoption or use. In addition, the Framework must include tools for transition planning as well as assessment tools for investment prioritization as part of the transition.

Recommended Questions for future RFIs on Cybersecurity Framework

1. **What considerations should be addressed in the area of "transition to and sustaining familiarization with the Cybersecurity framework?"**
2. **What sectors will not be impacted by the Framework, and how does "sector," and its authoritative definition, relate to NIST subject areas?**
3. **What are the provisions for assessing and detecting second- and third- order effects (i.e., unintended consequences) stemming from development, implantation and/or adoption of the framework?**

Contact Information

Frank Knickerbocker
Manager, Enterprise Management Division
ANSER
frank.knickerbocker@anser.org
703-416-3354