Views on the Framework for Improving Critical Infrastructure Cybersecurity

Multi Association Response
NIST RFI Issued: 12/11/2015

February 19th, 2016

Request for Information (RFI) Issued: 12/11/2015
Department of Commerce
National Institute of Standards and Technology (NIST)
Docket Number: 151103999-5999-01

Via cyberframework@nist.gov

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, M.D. 20899

Subject: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

We want to thank NIST both for the opportunity to respond to the Request for Information and the ongoing excellent work that NIST provides in working with the private sector to improve the nation's cyber security. The initial NIST Framework for cyber security has not only proven to be a useful tool in enhancing the nation's preparedness and resilience, but the process NIST employed in developing the Framework is a model for partnerships between government and industry.

Since the release of the Framework in February 2014 we have heard numerous accounts of organizations using and adapting the Framework to enhance their management of cyber risk and improve information sharing and communications processes across business structures and functions. In addition, other closely aligned tools such as the Department of Energy's C2M2 have been aligned with the Framework and have greatly benefitted particular critical infrastructure sectors.

While we view the development of the NIST Framework as a significant, and world-leading, step toward a sustainably secure cyber system, we agree that our work together on this topic is far from complete. We therefore welcome your initiative in launching the RFI to advance the effort.

Recognizing the inherently limited time and resources that infrastructure owners/operators and government have to address the cyber security challenge, we collectively urge the next phase of NIST's effort to focus on two central issues.

First, while many larger or more mature organizations have reported use of the Framework to validate or refine the processes they already have in place, we estimate that usage may have been lower for less mature and/or smaller entities. We are keenly aware of how critical it is for us to reach smaller entities as we operate in an interconnected system where even large and cyber aware elements of the critical infrastructure can be compromised by vulnerabilities regardless of an entities size. We, of course, support aggressive out-reach campaigns by critical infrastructure sectors, their trade organizations, and government partners to increase awareness of the Framework in organizations of all sizes, however it is apparent that these sort of outreach programs must grow and broaden. We urge the next phase of the

Framework set understanding the issues confronting theses smaller entities and addressing their unique concerns as a top priority.

Second, we need to reinforce the voluntary nature of the NIST Framework. One of the most visionary elements of the President's Executive Order that called for the Framework, and of the Framework itself, is the commitment to maintain a voluntary approach. As you know, both the cyber technology and the cyber threat methods change constantly and the President's Order wisely recognized that the traditional regulatory model is inadequate to address the ever evolving cyber landscape. In fact, backward facing "check the box" compliance regimes not only fail to enhance security but also detract from effective application of cyber security resources, risking a progressive debilitating of security for the sake of compliance.

Notwithstanding the clear vision and intent of both the Order and the Framework we are already experiencing instances of regulatory efforts that would turn the Framework into a compliance-based system. We are extremely concerned that that such regulatory misalignment could undermine the positive effects of the Framework by undercutting the collaborative nature of the partnership which we believe is absolutely critical to make and sustain significant strides toward the nation's cyber security goals.

We believe there is an opportunity for NIST, which understands the process and the substance of the Framework, to work with the private sector, as well as broader government interests, to assure that the intent, objectives, and vision of the Framework are appropriately realized.

We urge NIST to essentially replicate the process it used in developing the Framework with a renewed focus, not on expanding or refining the substance of the Framework, but working collaboratively with critical infrastructure sectors to promote appropriate use of the Framework.

Specifically, we suggest NIST work with us to fulfil the elements of the Executive Order that the President included to spur voluntary use of the Framework, but remain to be fulfilled. The topics we suggest be addressed are:

- Prioritization ---Smaller entities in particular have reported being confused and even overwhelmed by the size and complexity of the current Framework. An element of the next NIST process should examine this issue and attempt to find the best way to make the Framework more user-friendly for small and mid-sized entities.

- Cost Effectiveness --- Smaller entities, particularly in the private sector, are often challenged as they have to decide where to invest limited marginal capital available for information technology and cyber security enhancements. An element of the next NIST process should examine this issue with a goal of developing methods for which entities of varying sizes and resource bases could best assess which of the array of objectives and actions embedded in the Framework are best for their own particular company.

Identifying best practices based on lessons-learned will diminish the perceived need for regulation as businesses deploy processes that have effective in impact and cost.

- Incentives --- The President's Order called for development of incentives to promote broad and effective use of the Framework. As the National Infrastructure Protection Program points out there is a legitimate difference between commercial level of security and the national level of security. Moreover in cyber-attacks, non-governmental entities are often on the front lines. As a result, we need to find ways to encourage cyber sustained investments that build capacity to meet continuously evolving threats. A focus of the next NIST initiative could include methods and analyses identify incentives that can be deployed to promote the appropriate level of security in the national interest on a sustainable basis.

- Governance --- One of the assumptions of the NIST Framework is that it is a private sector led and government facilitated process that at some point would be managed by the sector stakeholders. An additional area of inquiry for the next NIST process could evaluate potential future governance models and examine their feasibility. Such evaluation should include NIST keeping the governance of the Framework rather than transitioning it to another organization.

- International Alignment – The global nature of cybersecurity risk calls for an approach that transcends national boundaries. The NIST Framework has already influenced risk management activities and discussions among domestic enterprises. Many of these companies have global operations and disparate regimes create confusion and inefficiencies. In this upcoming phase, NIST should evaluate what has been accomplished at the international level and how best to build upon some early success.

Again, we thank NIST for the leadership it continues to provide in working with the private sector and helping enhance our nation's cyber security. We collectively stand ready, willing and able to assist NIST in fulfilling the objectives we have outlined above.