February 23, 2016

Via cyberframework@nist.gov

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

RE: IT SCC Comments in response to NIST RFI – "Views on the Framework for Improving Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt:

The Information Technology Sector Coordinating Council (IT SCC) [1] would like to thank NIST not only for the opportunity to respond to your Request for Information, but for the continually excellent work NIST has done, and continues to do, in working with the private sector to improve our nation's cybersecurity. The initial NIST Framework for cybersecurity has proven to be a useful tool in enhancing our preparedness and resilience, and we commend the process by which NIST developed the Framework. In this spirit, we encourage NIST to continue advising other Federal agencies on appropriate and beneficial uses of the Framework. NIST should continue to promote use of the Framework as a voluntary, risk management tool, as envisioned by Executive Order 13636. However, in those instances where sectors are subject to current cybersecurity regulatory regimes, the Framework should be used as an orientation point around

[1] The IT SCC is comprised of nearly 100 diverse organizations from across the information technology sector. While this submission reflects our consensus views, we note that several of our members have submitted individual comments, which we urge NIST to consider as well.

which to align and streamline such existing regulatory efforts – not as a rationale for creating additional layers of regulation.

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 to improve communications between IT departments and the rest of organizations' business structure regarding the critical process of managing cyber risks. These anecdotes are testimony to the effectiveness of the process which NIST and the private sector employed in co-developing the Framework.

Recognizing the inherently limited time and resources both industry and government have to address the cybersecurity problem, the IT SCC urges the next phase of NIST involvement to focus on the following central issues:

- Clarifying the Framework Core
- Framework Guidance
- Global Framework Promotion
- Governance
- Incentives

We view the development of the NIST Framework as a significant, and world-leading, step toward a sustainably secure cyber ecosystem, yet our work together on this topic is far from complete. Pursuant to NIST's authority under the Cybersecurity Enhancement Act of 2014 to facilitate and support the development of voluntary, consensus-based, industry-led best practices such as the Framework, we welcome your initiative in launching this next phase of the Framework process, including the RFI and upcoming Workshop, to help move us further down this path.

Clarifying the Framework Core

The Framework's core is a helpful structure for developing risk management processes, stimulating useful processes across organizations, and establishing relatable benchmarks both internally and externally. But the simplicity of the Framework sometimes limits its use across more complex organizations. For example, establishing current and target profiles is a useful activity; however, there is little available guidance regarding how to examine, use, or reconcile multiple current or target profiles. Similarly, the text of the implementation tiers sometimes creates overlapping metrics, which may lead to subjective risk determinations. While flexibility is certainly key, particularly as organizational risk objectives vary greatly, promoting certainty and confidence in decision making are also important goals. Developing greater clarity around what distinguishes one tier from another could provide a more useful frame of reference for many Framework users.

In addition, risk management standards, as well as the threat environment itself, are constantly evolving. Accordingly, the list of informative references should be reviewed and updated on a periodic basis. Within this construct, the IT SCC believes the focus of NIST and the broader stakeholder community should be on refining and clarifying the Framework, not expanding it.

It also bears mentioning that, as pointed out in the Roadmap for Improving Critical Infrastructure Cybersecurity (the "Roadmap") NIST published concurrently with the Framework, important work needs to be done in areas not currently included in the Framework, such as authentication and supply chain risk management. We believe it is still premature to incorporate topics such as these in the Framework, in particular due to the lack of developed consensus-based, industry-led international standards and best practices in these areas. We encourage NIST to continue working with stakeholders to help promote development of standards in these areas, something we note NIST is already doing in other contexts, such as in the recently published "Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity," which helpfully noted the lack of developed cybersecurity standards in several important areas.

Framework Guidance

The use of the NIST Framework is still in the preliminary stages. Not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity – such as the Framework – to appropriately balance cyber risk. Smaller companies in particular have reported being confused and even overwhelmed by the size and complexity of the current Framework. Given the interconnected nature of the cyber ecosystem, we are keenly aware that cyber elements of the critical infrastructure can be compromised by weaknesses in smaller entities to which they are technologically connected. By way of illustration, reportedly a recent breach of a large corporate retailer was facilitated by a compromise to the retailer's HVAC vendor. Given that smaller connected entities in larger companies' ecosystems can serve as attack vectors, it is critical for us to create a sustainably secure cyber ecosystem across all entities, large and small. Therefore, in the next phase of Framework development, we recommend that NIST work with interagency partners including DHS, the Small Business Administration, and Sector Specific Agencies to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and consider ways to make the Framework more approachable for all organizations. NIST should prioritize understanding the issues confronting theses smaller entities and addressing their unique concerns and needs.

The goal of such guidance efforts, simply stated, is to help make it easier for a broader diversity of organizations to use the Framework. These practices could help organizations better assess how the array of actions embedded in the Framework can best be leveraged to meet the requirements and risk tolerances of organizations of various sizes across numerous industry segments. With this knowledge in hand, and by also factoring in business needs including cost effectiveness, organizations may be more likely to adopt processes they know they can afford and are more readily applicable to their particular risk environments.

Global Framework Promotion and Alignment

As a sector, we have supported organizations across the globe who are using the NIST Cybersecurity Framework as the basis to assess their actual cybersecurity risks. The Framework is gaining traction internationally, and familiarity is growing in multiple geographies. Specifically, international use of the Framework is gaining support in the following sectors: Financial, Electric Utilities, Water Utilities and Oil and Gas. Furthermore, the Framework is being used to establish security requirements and as a way to recommend threat mitigation controls and remediation. Promoting the Framework in its current form will help enable the US to sustain its leadership on cybersecurity around the world, and doing so will in turn help to further enhance its use within the United States.

Domestic Framework Alignment

As a starting point, NIST should work with its interagency partners to drive alignment of cybersecurity requirements for Federal information systems with the cybersecurity outcomes of the Framework. A majority of information security vendors service both the public and private sectors. Aligning Federal Information Security Management Act requirements with the Framework subcategories, and mapping these requirements to other global standards referenced in the Framework will enable more vendors to compete in the public and private sector information security marketplaces, driving further innovation and improving security capabilities.

Global Framework Promotion

NIST and its Federal agency partners should also promote these approaches with their global government partners. For example, the Department of State should reference the Framework in all of its global cybersecurity capacity-building efforts. Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships. International acceptance of industry-led, global cybersecurity standards allows for even greater competition and innovation in the marketplace.

Governance

Since the publication of the Roadmap in February 2014, NIST has consistently raised the question of whether governance of the NIST Framework should be transitioned to a private sector organization. For now, we recommend that NIST, as a non-regulatory federal entity with expertise in convening diverse stakeholders, continue to play a leadership role in the promotion and maintenance of the Framework. However, given NIST's demonstrated interest in this topic, perhaps NIST can engage with the private sector to drive more focused discussions concerning options for long-term governance of the Framework.

Incentives

Over the past two years, the Departments of Homeland Security, Commerce, and Treasury have each conducted studies and published proposals, in accordance with EO 13636, with recommendations on incentives such as the use of grants, rate recovery for price regulated industries, cybersecurity insurance, and public recognition, among others, to encourage further voluntary use of the Framework. We encourage USG stakeholders including NIST to continue their work on incentives. Examples of incentives worthy of further exploration may include an optional public recognition program based on and incorporating programs that already exist within, or will be developed by, the private sector; the use of government procurement considerations to encourage the adoption of cybersecurity standards; and continued engagement with insurance companies to explore ways that cybersecurity insurance might incentivize companies' use of the Framework. The effective use of incentives would help businesses of all sizes, and in particular, SMBs, justify the costs of investments in cybersecurity and promote greater use of the Framework.

Conclusion

We again want to thank NIST for the leadership it continues to demonstrate in working with the private sector to help enhance our nation's cybersecurity. We stand ready, willing and able to assist NIST in fulfilling the objectives we have outlined above, and look forward to continued engagement with you to advance our shared goal of improving global cybersecurity.

Sincerely,

John Miller
IT SCC Chair