January 19, 2018

*Via Electronic Filing (cyberframework@nist.gov)*

**Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology on the *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Draft 2*.**

## I. INTRODUCTION

The Telecommunications Industry Association ("TIA") respectfully submits these comments in response to the National Institute of Standards and Technology's ("NIST") Request for Comment ("RFC") on its second draft update ("Version 1.1 Draft 2") to the Framework for Improving Critical Infrastructure Cybersecurity ("Framework" or "CSF").[1] TIA deeply values NIST's commitment to an inclusive process in its continued dialogue with Framework stakeholders.

As both a standard setting body and advocacy organization, TIA represents hundreds of manufacturers and vendors of information and communications technology ("ICT") equipment and services supplied to critical infrastructure owners and operators across the globe, enabling secure and resilient network operations across myriad segments of the economy.[2] TIA has participated in NIST's process since the Framework's inception and is pleased to see the Framework continue to gain popularity as an invaluable resource for cybersecurity risk management across sectors and internationally. TIA and its members look forward to continued partnership on this initiative as we reaffirm commitment to a voluntary, consensus-based, industry-driven approach.

As Framework users begin to consider the updates incorporated into Version 1.1 Draft 2, TIA encourages NIST to focus on increased outreach and education, developing more use cases – particularly for small and medium size businesses – and collaborating with international stakeholders so that the Framework can further its mission of providing a common language for cybersecurity risk management.

## II. TIA SUPPORTS THE BROADENING APPLICATION OF THE FRAMEWORK

In the few years since its publication, the tangible, voluntary nature and utility of the Framework has led to its use beyond the scope of the critical infrastructure organizations for which it was originally conceived. Such use is indicative of the success of the Framework as a burgeoning cybersecurity risk

[1] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Draft 2, Request for Comments, ("Version 1.1 Draft 2").

[2] Additionally, TIA writes and maintains voluntary industry standards and specifications, as well as formulates technical positions for presentation on behalf of the United States in certain international standards fora. TIA is accredited by the American National Standards Institute (ANSI) to develop voluntary industry standards for a wide variety of telecommunications products and sponsors more than 70 standards formulating committees. These committees are made up of over 1,000 volunteer participants, including representatives from manufacturers of telecommunications equipment, service providers, and end-users – including the United States government. Member companies and other stakeholders participating in the efforts of these committees and sub-groups have produced more than 3,000 standards and technical papers that are used by companies and governments to produce interoperable products around the world.

management tool. TIA therefore supports NIST's clarification in Version 1.1 Draft 2 that the Framework may be useful broadly to "organizations relying on technology, whether their cybersecurity focus is primarily on information technology ("IT"), industrial control systems ("ICS"), cyber-physical systems ("CPS"), or connected devices more generally, including the Internet of Things ("IoT")."[3] As TIA supports and encourages broad use of the Framework however, it is ever more imperative that stakeholders protect its voluntary, flexible nature so that we can continue to build the Framework as a resource rather than rue an anachronistic restraint. TIA appreciates NIST's commitment to this goal and looks forward to driving awareness of the Framework as a resource for organizations relying on a broad array of technologies.

## III. TIA SUPPORTS CHANGES TO SECTION 4.0 ON RISK MEASUREMENT

As TIA indicated in comments on the previous draft Version 1.1, tying the Framework too narrowly to measurements and metrics could damage the Framework's careful balance between the development of meaningful communication tools and the need for a flexible, voluntary risk management process.[4] Worse, such language could accelerate the natural tendency for flexible risk management approaches to develop over time into compliance checklists. TIA therefore applauds the amendment of Section 4.0 in Version 1.1 Draft 2 from "Measuring and Demonstrating Cybersecurity" to "Self-Assessing Cybersecurity Risk with the Framework" in a manner that is consistent with the Framework's overall approach and goal as a valuable industry resource. The revised language, which reflects the findings of considerable stakeholder research, discusses metrics and measurements as an important tool for enterprises to gage their own risk management internally and work to achieve organizational objectives. TIA and its members support the ability of organizations to effectively measure and communicate their own risk posture through a dynamic process and value NIST's commitment to this goal.

TIA appreciates Version 1.1 Draft 2's emphasis that "[o]rganizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management."[5] As the configuration of networks and technologies continues to rapidly shift and develop, the ability for organizations to "innovate and customize how they incorporate measurements" into their risk assessment will be increasingly vital.[6] The clarified language in Section 4.0, consistent with the flexible and voluntary nature of the overall Framework, will help prevent the ossification of ill-fitting measurement check-lists and foster collaborative, evolving approaches to better face the challenges ahead.

## IV. TIA SUPPORTS REFINEMENTS ON SUPPLY CHAIN RISK MANAGEMENT AND ENCOURAGES FOCUS ON INTERNATIONAL OUTREACH AND RESOURCES FOR SMALL BUSINESSES

[3] Version 1.1 Draft 2 at 2.
[4] *See* Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity (Docket No. 130208119-3119-01).
[5] Version 1.1 Draft 2 at 21.
[6] *Id.* at 22.

TIA appreciates NIST's focus on the importance of communication between stakeholders in managing risk between interdependent organizations. To aid in this communication and its efficacy, TIA urges NIST to be careful in maintaining flexibility in the supply chain risk management ("SCRM") process as well as to prioritize international outreach and Framework resources for small organizations.

In an increasingly complex ecosystem of infrastructure and devices, the practices of players across the full ICT supply chain impact the risk posture of those with whom they connect. As NIST notes in Section 3.3, "[s]upply chains are a complex, globally distributed, and interconnected set of resources and processes between multiple levels of organizations." As TIA has also noted, effective SCRM is profoundly complex and many organizations face challenges beyond their control. Many organizations' supply chains include hundreds of vendors, spanning numerous countries with disparate risk management approaches and norms. Effective SCRM will require long term international collaboration as industry works to develop standards and best practices as well as use of those best practices by both large and small entities. As users of the Framework begin to consider Section 3.3 on Communicating Cybersecurity Requirements with Stakeholders and ID.SC among other elements of the Framework, stakeholders must remain vigilant in avoiding approaches to SCRM that could develop into an ineffective compliance checklist and NIST should prioritize aiding small businesses in achieving their organizational goals.

## V. TIA SUPPORTS NIST'S ROADMAP DRAFT UPDATE AND CAUTIONS AGAINST PRESCRIPTIVE MEASUREMENT

TIA applauds NIST's continued commitment to the goals and activities outlined in the 2014 NIST Roadmap for Improving Critical Infrastructure Cybersecurity and generally supports additions made in the Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1.[7] TIA particularly appreciates NIST's work in promoting the Framework internationally as outlined in Section 4.8 as well as its aim to build awareness among, and resources for, small businesses as outlined in Section 4.12.[8]

We appreciate NIST's intent to research and provide resources regarding cybersecurity measurement as indicated in Section 4.9.[9] However, while TIA values and recognizes the importance of measurement in risk assessment, we caution NIST against over-standardization of cybersecurity measures. As stakeholders have noted before, to effectively manage risk organizations must be able to tailor measurement systems to fit their needs and modify those systems as the needs of the organization change over time. As NIST looks at "aligning technical measures to determine effect on high-level organizational objectives" and "support decision making by senior executives and oversight by boards of directors," it should remain vigilant in maintaining the divide between informative research and fundamentally changing the Framework itself.[10]

---

[7] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, NIST (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf; *Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1*, NIST (Dec. 5, 2017) ("Roadmap Draft Update").
[8] Roadmap Draft Update at 13-14, 17-18.
[9] *Id.* at 14-15.
[10] *Id.*

## VI. CONCLUSION

TIA thanks NIST for its public request for stakeholder input on the second draft update of the Framework and we look forward to continued partnership with NIST as well as the broad community of Framework stakeholders on this important work.

Respectfully submitted,

**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

By: /s/ *Savannah P. Schaefer*

Savannah P. Schaefer
Policy Counsel, Government Affairs