ADVANCING GLOBAL COMMUNICATIONS
TIAONLINE.ORG

April 10, 2017

Via Electronic Filing (cyberframework@nist.gov)

Re: 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)

I. INTRODUCTION

The Telecommunications Industry Association (TIA) submits these comments in response to the National Institute of Standards and Technology's (NIST) Notice and Request for Comments (RFC) seeking feedback on its Draft Update to the Framework for Improving Critical Infrastructure Cybersecurity (Framework).[1] TIA appreciates NIST's commitment to an inclusive approach through continued outreach to stakeholders and efforts to collect information regarding the use and efficacy of the Framework.

As both a standard setting body and advocacy organization, TIA represents hundreds of global manufacturers and vendors of information and communications technology (ICT) equipment and services that are supplied to critical infrastructure owners and operators, enabling secure and resilient network operations across segments of the economy.[2] As NIST works to include supply chain risk management (SCRM) and risk management metrics and measures into the scope of the Framework, TIA looks forward to continued partnership in building a common language for cybersecurity policy and process.

In order to foster an effective, adaptive and ever-improving set of cybersecurity protections, the Framework must remain vigilant in its commitment to a flexible, voluntary, and consensus-based approach.

II. TIA RESPONSES TO QUESTIONS POSED IN THE UPDATE MARKUP

a. Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

[1] National Institute of Standards and Technology, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, Notice and Request for Comments, 82 Fed. Reg. 8408 (Jan. 25, 2017) (RFC).

[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.

Though still in its early years of implementation, the Framework already accommodates a wide variety of organizations' differing cybersecurity needs across the broad landscape of the economy. Before expanding further beyond the new areas proposed in the draft, the Framework needs more time to gain widespread use and prove itself in various parts of the market. TIA members have expressed support for the Framework and relate positive experiences where they have used it. TIA supports continued efforts to increase awareness and use of the Framework as the common language of, and model playbook for, a voluntary risk management approach that is dynamic and flexible.

b. How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

With the addition of section 4.0 "Measuring and Demonstrating Cybersecurity," the updated draft explains the inclusion of "Framework measurement" as a means for organizations "to understand and convey meaningful risk information to dependents, partners, and customers" therein providing "a basis for strong, trusted relationships, both inside and outside of an organization."[3] TIA recognizes the importance of forging this trust through the exchange of meaningful information among partners.

To date, the Framework has carefully balanced the development of meaningful communication tools with the need for a flexible, voluntary process of risk management. Tying the Framework too narrowly to measures outlined in the Framework's Informative References could potentially damage this balance, or worse, could accelerate the natural tendency of flexible approaches to risk management to develop over time into compliance checklists. As the update notes, "[t]he ability of an organization to determine cause-and-effect relationships between cybersecurity and business outcomes is dependent on the accuracy and precision of the measurement systems" and "[t]herefore, the measurement systems should be designed with business requirements and operating expenses in mind."[4] In order for organizations to successfully tailor measurement systems to fit their needs, a focus on metrics for metrics' sake could be counter-productive. Instead, an organization must first identify a *methodology* of risk management measurement that suits its particular circumstances; the specific metrics the organization may choose to use in its risk management should derive from the methodology that is best suited to that organization's particular needs.

In all cases, we must vigilantly protect the Framework's flexible and voluntary nature against the tendency of metrics to ossify into one-size-fits-all mandates. The Framework's guiding principles of collaboration and flexible risk management are well-suited to helping stakeholders and individual organizations develop risk management measurement methodologies that provide for dynamic and ever-improving risk management.

Likewise, the practices of various players in the ICT supply chain bear heavily on the cybersecurity outcomes of the end user. TIA applauds the consideration of SCRM in the body of the Framework. Effective SCRM, however, is a profoundly complex and difficult endeavor and many organizations face challenges beyond their control. The global nature of ICT supply chains requires international and industry-driven best practices and standards. As with risk management measurement, we applaud the effort to advance SCRM through the draft Framework update, while we also caution that

[3] Framework Update at lines 744-747.
[4] *Id.* at 762-765.

stakeholders in this process should be vigilant to avoid SCRM approaches that could over time develop into an inflexible compliance checklist.

TIA believes the processes for developing meaningful risk management measurement and SCRM are nascent, and we look forward to exploring strategies for effective metrics methodologies and SCRM in NIST's forthcoming workshops. To that end, we propose that the workshop in May take an affirmative focus on the question of how to develop meaningful metrics and SCRM that remain flexible and dynamic rather than leading to a compliance checklist approach.

c. Based upon this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

TIA applauds NIST's commitment to the goals and activities outlined in the 2014 NIST Roadmap for Improving Critical Infrastructure Cybersecurity (Roadmap).[5] NIST's continued efforts to promote awareness of cybersecurity risks and the utility of the Framework is driving adoption of the Framework and better cyber hygiene across public and private sectors alike.

III. CONCLUSION

TIA thanks NIST for its public request for stakeholder input on the drafted update of the Framework. The ICT community looks forward to the workshop in May and continued work with NIST as it moves forward.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Cinnamon Rogers*

Cinnamon Rogers
Vice President, Government Affairs

Savannah Schaefer
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road, Suite 200
Arlington, VA 22201
(703) 907-7700

[5] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, NIST, (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf.