TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

February 23, 2016

Via Electronic Filing (cyberframework@nist.gov)

Re: National Institute of Standards and Technology's Notice and Request for Information, *Views on the Framework for Improving Critical Infrastructure Cybersecurity* [Docket No. 151103999–5999–01]

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

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 Information ("RFI") seeking information about the ways the NIST Cybersecurity Framework ("Framework") is being used and how best practices for using it are being shared.[1] TIA appreciates NIST's commitment to an inclusive approach through continued outreach to stakeholders and efforts to collect public input on usage and perception of the Framework, to date.

TIA is a trade association representing 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. We offer the specific input below based on TIA efforts to raise awareness of the Framework and our members' experience using it.

[1] National Institute of Standards and Technology (NIST), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, 80 Fed. Reg. 76934 (Dec. 11, 2015) ("RFI").

II. USE OF THE NIST CYBERSECURITY FRAMEWORK

TIA commends NIST for its efforts to not only advance the Framework but assess its value and usefulness to all stakeholders. We appreciate NIST's engagement in a transparent process during the development of the Framework as well as the post-publication initiatives aimed at educating relevant communities about the Framework and facilitating its adoption. At this stage, two years since its initial publication, the Framework serves as an important tool to aid industry in developing a common language and approach for dealing with cyber risks.

While the Framework is still in its early stages, TIA believes there is increasing general awareness of the Framework amongst TIA members and the ICT manufacturer and supplier community as a whole. Additionally, TIA members have expressed support for the Framework and have reported positive experiences where it has been adopted. TIA has helped facilitate this by promoting awareness of the Framework amongst the ICT community and by advocating it as the model for a voluntary cyber risk management approach.

TIA has worked to share developments related to the Framework with member companies through its Cybersecurity Working Group, which determines the association's public policy positions related to the security of ICT equipment and services from a vendor perspective as it relates to critical infrastructure, supply chain, and information sharing. This includes informing members of NIST's activities regarding the Framework itself as well as the Department of Homeland Security's Critical Infrastructure Cyber Community (C^3) Voluntary Program, which is intended to support industry in increasing its cyber resilience; increase awareness and use of the Framework; and encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

Awareness amongst TIA's membership has also been driven by TIA's continued work related to the Framework. Most directly, TIA has worked to raise awareness of the Framework as it worked with NIST to provide ICT industry consensus views towards finalizing the Framework. Since the Framework was finalized, TIA has continued to work with its members on efforts and issues related to the Framework that have increased awareness including attendance at NIST Framework events and providing input on the initial RFI seeking input on

Framework awareness. Additionally, TIA was an active member of the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 4, which was an effort to map the Framework to the communications sector. Further, TIA is a member of the Communications and IT Sector Coordinating Councils, key venues for receiving information and sharing lessons learned about the Framework and other network reliability and resiliency issues generally. Besides our policy-based efforts to share information with members, TIA also engages in standards-based activities and coordination with other industry associations to spread the value of the Framework to industry and government stakeholders.

Furthermore, as communications technologies are increasingly being incorporated in other industry segments and products, beyond traditional critical infrastructure, government entities as well as the public at large are starting to consider issues surrounding cyber threat readiness in these sectors. TIA and its members have identified the Framework as a great model for consideration of how to begin developing a flexible, voluntary, viable mechanism for cybersecurity readiness and resilience. For example, in response to a U.S. Department of Transportation request for comment on Automotive Electronic Control Systems Safety and Security, TIA encouraged the agency to align its cybersecurity risk management efforts with existing guidance documents done through public-private partnerships like the Framework.[2] In addition, TIA's white paper on "Realizing the Potential of the Internet of Things: Recommendations for Policy Makers,"[3] which addresses policy approaches for dealing with Internet of Things security, specifically identifies the Framework's voluntary, risk-based, and technology neutral methodology as one that lawmakers should look toward when considering cybersecurity implications for the Internet of Things rather than adopting rigid standards or mandates.

---

[2] *See* TIA Comments, NHTSA-2014-0108, at 4-5, *available at* https://www.tiaonline.org/sites/default/files/pages/Automotive_Electronic_Systems_Security_Comment_Final.pdf.

[3] *See* TIA White Paper, *Realizing the Potential of the Internet of Things* at 9, http://www.tiaonline.org/sites/default/files/pages/TIA-White-Paper-Realizing_the_Potential_of_the_Internet_of_Things.pdf.

This demonstrates that TIA members and the larger ICT industry have increased recognition of the value of the Framework's approach, are taking steps to promote it, and that many companies have begun to apply its methodology to their individual business models. For those that have begun to use the Framework, however, there may be proprietary and/or competitive concerns associated with this fact or the results of the use of the Framework so far. TIA, therefore, believes that NIST should not attempt to measure the effectiveness of the Framework from the results of this RFI, and defers to individual companies to provide more specific input about their initial experiences with the Framework, should they wish to provide this information.

III. AREAS OF POSSIBLE IMPROVEMENT FOR THE FRAMEWORK

As we have previously noted, the Framework is still in the initial stages for usage and adoption. Thus, TIA and its members strongly believe it would be premature for NIST to pursue significant updates to the methodology and approaches outlined in the Framework. The ICT community is just at a point of being more adept with the Framework and many have only recently begun to implement its approach. Therefore, we believe that it would not be advantageous at this time to pursue a process for updating framework for cybersecurity as industry is just at a point of using and recognizing the Framework's value.

Instead, TIA encourages NIST to focus the next stage of Framework development on areas where further work is needed towards the goal of promoting the Framework's voluntary, industry-led methodology as the most effective approach for enabling industry to adopt practices that will aid in their cyber infrastructure security, resiliency, and responsiveness. The objective should be continuing to use the Framework to reinforce the idea that voluntary, process-oriented guidelines, developed with industry's input, of the kind embedded in the Framework is superior to mandated cybersecurity standards. Specifically, NIST should work on promoting the elements of the Framework domestically, with civil agencies at the Federal and state levels, as well as on the international front.

Internationally, awareness of the Framework has continued to increase, particularly amongst the community of subject matter experts. In an increasing number of jurisdictions,

where alternative mandate-based approaches are sometimes proposed, policymakers are becoming more aware of the existence of the Framework as it begins to be more widely used across Critical Infrastructure/Key Resource (CIKR) sectors within the United States. Nonetheless, NIST along with its government counterparts could do more to advance the Framework itself as well as the following U.S.-supported principles that led to the successful Framework model:

- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain;
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure; and
- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging cyber threats.

This type of international engagement will be crucial to ensuring there is global harmonization on addressing cyber threats. Such an approach is necessary to ensure that the ICT industry can develop the most efficient, effective security protocols rather than region- or country-specific policies.

TIA and its members believe that global harmonization of standards and best practices is critical as the ICT industry operates in a global marketplace where sector-specific rules can serve as barriers to trade and significantly inhibit the continued growth of the industry. The importance of harmonized approaches is particularly important in the area of cybersecurity, where the United States is already a leader in adopting a flexible, public-private approach. Therefore, TIA believes the federal government must embrace this role and work to enhance its role as the standard-bearer in the cybersecurity space. We applaud the Administration's recent efforts towards achieving this goal. We believe the 2015 report outlining a new strategy to improve the U.S. government's engagement in the development of international cybersecurity standards sets us on the right track and has a number of important recommendations.[4]

[4] *See* The White House Blog, "Engaging the International Community on Cybersecurity Standards," Dec. 23, 2015, https://www.whitehouse.gov/blog/2015/12/23/engaging-international-community-cybersecurity-standards. TIA

Furthermore, in the recently passed Cybersecurity Act of 2015, section 402 directs the Department of State to develop a comprehensive cybersecurity strategy relating to United States international policy with regard to cyberspace.[5] TIA and its members believe this initiative would serve as an ideal avenue for the Administration to incorporate the Framework's key principles and develop a larger plan for promoting this approach on a global scale. We encourage NIST to coordinate with its counterparts in the State Department to educate them on the Framework and assist with formulating a strategy that has foreign adoption of the Framework as part of its objective.

IV. CONCLUSION

TIA thanks NIST for its public request for input on views and uses of the Framework and possible future areas of further development. The ICT manufacturing and vendor community stands ready to work with NIST as it moves forward.

Respectfully submitted,

By: */s/ James Reid*

James Reid
Senior Vice President, Government Affairs

Avonne Bell
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd, Ste 200
Arlington, VA 22201
(703) 907-7711

February 23, 2016

---

was also encouraged to see the recent cybersecurity announcements by the Administration and we hope that the new initiatives, including the newly established Commission on Enhancing Cybersecurity, will include recommendations about furthering use of the Framework particularly on the international front.

[5] Cybersecurity Act of 2015, Pub. L. No. 114-113, div. N, §402.