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

October 10, 2014

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

Adam Sedgewick
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

**Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology's Notice and Request for Information, *Experience With the Framework for Improving Critical Infrastructure Cybersecurity* (Docket No.: 140721609–4609–01)**

## I. INTRODUCTION AND STATEMENT OF INTEREST

The Telecommunications Industry Association (TIA) submits these comments to the National Institute of Standards and Technology (NIST) in response to its Notice and Request for Information relating to awareness of and initial experiences with the NIST Cybersecurity Framework (Framework).[1] TIA appreciates NIST's outreach to the public to collect input at this stage of the Framework's availability and in advance of the upcoming public Framework workshop.

TIA is a trade association representing hundreds of global manufacturers, vendors, and suppliers of information and communications technology (ICT) that supply countless owners and operators of critical infrastructure, enabling secure and resilient network operations

[1] NIST, *Experience With the Framework for Improving Critical Infrastructure Cybersecurity*, 78 Fed Reg 50891 (Aug. 26, 2014) (RFI).

across segments of the economy. Generally, through its Cybersecurity Working Group TIA engages in policy advocacy consistent with the following principles:

- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging threats.
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure.
- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain.
- Governments should provide more timely and detailed cyber intelligence to industry to help identify threats to protect private networks.
- Cybersecurity funding for federal research efforts should be prioritized.

We appreciate NIST's efforts and transparent process in the development of the Framework to date, and look forward to working with NIST on Framework-related activities moving forward, and offer the specific input below based on the consensus views of TIA's hundreds of ICT manufacturer, vendor, and supplier member companies.

## II. TIA COMMENTS ON AWARENESS OF THE NIST CYBERSECURITY FRAMEWORK

TIA believes that there is widespread awareness of the Framework amongst the members of the ICT manufacturer, supplier, and vendor community. 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. These include the activities of NIST in the development of 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. For example, TIA co-chairs an effort to define the communications sector ecosystem within the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 4 (Cybersecurity Best Practices), which has the goal of mapping the Framework specifically to the communications sector. Further, TIA is a member of both 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.[2] Other efforts, such as the QuEST Forum,[3] which is responsible for the TL 9000 telecom quality management standard, have served as valuable venues for NIST to

[2] For example, members of the CSCC, made up of broadcasting, cable, wireline, wireless, and satellite segments, have participated in multiple NIST, Department of Homeland Security (DHS), and industry association-sponsored programs, webinars, and panels with future events being planned.

[3] *See* http://www.questforum.org/.

directly share information with US and Canadian communications service providers and ICT manufacturers and vendors, as well as for those entities to collaborate with each other. TIA and its members remain committed to these public-private partnerships as a means for collaborating on current and emerging threats.

TIA continues to undertake efforts to increase awareness of the Framework within its membership through the sharing of information within its policy-based efforts as well as its standards-based efforts, and through educational videos and publications. The reach of TIA also extends to stakeholders generally as we make some of this information publicly available. TIA intends to continue to help increase awareness of the Framework moving forward, and to work to ensure that industry-driven best practices and global standards be relied upon to address the security of critical infrastructure across sectors. TIA also partners with other industry associations and other organizations to undertake these efforts.

TIA, with a membership comprised of ICT businesses of all sizes, understands and appreciates that small businesses are a crucial driver of the American economy yet may not generally have broad awareness of the Framework, nor have the resources to invest in the prevention of cyber attacks, to the degree that larger organizations do. For small businesses, the importance of education and public awareness in efforts to improve resiliency to cyber-based attacks is especially crucial. These educational efforts, ideally coordinated across the government, will aid small businesses in understanding cybersecurity threats, increase awareness of existing helpful resources available from the government, and help explain how these resources can be best utilized (e.g., how to use the NIST Framework).

Awareness of the Framework is a valuable and necessary step, but it is important that it be accompanied by a correct understanding of how to use the Framework. For example, TIA has observed that not all stakeholders are fully aware of the voluntary nature of the Framework. For instance, TIA has observed several attempts by policymakers to make use of the Framework mandatory, disregarding the nature of the Framework as a toolbox from which organizations may pull tools to aid in the development and/or enhancement of their particular cybersecurity programs as appropriate. Some of this confusion may also be due to requirements for the use of the Framework within Federal agency processes. We appreciate

NIST's adherence to the voluntary nature of the Framework prescribed in E.O. 13636, and urge that NIST continue to make clear that E.O. 13636 requires the incorporation of voluntary consensus standards and industry best practices, along with the reasons for this approach (such as consistency with the Office of Management and Budget's Circular A-119[4] and the National Technology Transfer and Advancement Act[5]).

As a further example, TIA has found that there is not a uniform understanding across stakeholders as to the scope of the Framework. Because the Framework is explicitly scoped to address critical infrastructure owners and operators (and not non-critical systems), it should remain a priority for NIST to clarify that while owners and operators of non-critical systems may benefit from the lessons learned through the use of the Framework by owners and operators of critical systems, the Framework is not intended to apply to non-critical systems.

Internationally, awareness of the Framework has also 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 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. TIA continues to emphasize to these governments that the most effective solutions ensure innovation by relying on voluntary use of internationally-accepted standards and best practices, and that neither the Framework nor any other government action should be used to implement cybersecurity policies that would restrict trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system. Moving forward, the U.S. Government itself should play a role in increasing awareness of the Framework through government-to-government discussions and other international fora.

---

[4] *See* OMB Circular A-119 Revised, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (rev. Feb. 10, 1998) *available at* http://www.whitehouse.gov/omb/rewrite/circulars/a119/a119.html.

[5] *See* 15 U.S.C. §3701 et seq. (1996).

## III. TIA COMMENTS ON INITIAL EXPERIENCES WITH THE NIST CYBERSECURITY FRAMEWORK

Initially, TIA notes that the Framework has only very recently been released, and that it is too early to be able to understand to what degree the Framework has helped organizations understand the importance of managing cyber risk. While some of TIA's members have begun to use the Framework to the extent appropriate, the ICT industry has not had time to widely apply it. Further, for those that have begun to use the Framework, some may have 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 input about their specific initial experiences with the Framework, should they wish to provide this information at this point in time.

In the RFI, NIST puts forward several questions that solicit input on the adequacy of the Framework's major components, and guidance provided in the Framework on how to use it.[6] Because there is not a developed methodology for how to calculate and apply Tiers, using the Tiers outside of an organization's risk management process runs the risk of false comparisons between organizations based on non-standard profiles. The same is true for Framework Profiles due to the lack of methodology for calculating a Profile making the external uses contemplated by the Framework in Section 3.3 imprecise, as there is no standard for measuring an organization's Framework Profile against other organizations' Framework Profiles. TIA has proposed to NIST that, in order to avoid these imprecise comparisons, NIST should make clear that for the purposes of Version 1.0 of the Framework, Profiles and Tiers should be to aid internal risk management processes (and not for external metrics). As NIST develops the next version of the Framework in the future, NIST could develop a methodology for calculating and applying Profiles and Tiers so that the results can validly be used for information and comparison outside of organizations. The development of use cases will also be essential to the wider use of the Framework.

[6] RFI at 50893.

Specific to the communications sector, with the FCC CSRIC's Working Group 4, an effort exists to map the Framework to the communications sector, which TIA is a supportive member of on behalf of the ICT manufacturer, vendor, and supplier community. This Working Group's effort is to buoy assurance of reliability and resilience for core public communications functions that are confronted by cyber-based threats by developing voluntary tools which can be used to ensure that communications providers take needed steps throughout their processes to manage these cybersecurity risks, through demonstrating how communications providers can apply the Framework. The work also includes the development of use cases for segments of the communications sector, and the planned completion of this effort is March of 2015. Further, TIA notes that Working Group 4's official description states that these assurances:[7]

(1) can be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., not one-size-fits-all);

(2) are based on meaningful indicators of successful (and unsuccessful) cyber risk management (i.e., outcome-based indicators as opposed to process metrics); and

(3) allow for meaningful assessments both internally (e.g., CSO and senior corporate management) and externally (e.g., business partners).

From a practical perspective, TIA's members already work with their customers, including CIKR owners and operators across sectors, to provide products and services that are responsive to the ever-changing security needs driven by demands for business continuity and competitive differentiation. TIA believes that it is very important for NIST and other policymakers to incorporate into their considerations and activities related to the Framework the need to connect risk management practices with business decisions impacted by compliance evaluation requirements. For example, the upcoming NIST-hosted Framework workshop would be an excellent forum for this aspect to be discussed publicly.

In practice, the ICT vendor community could be impacted in situations where a network owner or operator has outsourced some or all of its operations, or in certain trusted

[7] *See* CSRIC IV Working Group descriptions, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_9_2_14.pdf.

relationships between owners/operators and their vendors where the ability of the owner/operator to provide critical infrastructure services is directly impacted by their vendor's business continuity. However, as a result of the early stage of the Framework's use, TIA is not yet able to provide a conclusive view on the effect the Framework will have as a result.

## IV. TIA VIEWS ON THE FRAMEWORK'S ROADMAP

In the RFI, NIST requests input on its NIST Roadmap for Improving Critical Infrastructure Cybersecurity, including on whether there are key issues or opportunities missing from it.[8] In response, TIA urges NIST:

- that inclusion of Federal agency cybersecurity alignment is supported by TIA as part of the Roadmap, and should be a cornerstone of any future Framework-related activities by NIST;
- that the Roadmap presents the opportunity to include consideration of important economic considerations and their linkage to risk management decisions to address cyber-based threats which range from low/moderate to highly sophisticated, and how these relate to the most critical functions and data of an organization;
- to continue to prioritize the scope of the Framework as applying to the owners and operators of critical infrastructure, prescribed in E.O. 13636, and not non-critical systems;
- the Framework should not serve as the foundation for conformity assessment because it is not a security requirement or standard that provides a methodology to be used to determine whether something is in conformance or not. As NIST has made clear, the Framework is a "toolbox" that organizations can use the degree determined to be appropriate;
- that any activity related to supply chain risk management fully appreciates the international nature of the ICT industry which requires a global approach to address

[8] RFI at 50893.

cybersecurity concerns, and that a global supply chain can only be secured through an industry-driven adoption of commercially practical best practices and global standards embracing that reality. In particular, mutually recognized international agreements are particularly useful in that they enable ICT manufacturers to build once and then sell globally; and

- consistent with our views previously communicated to NIST on the roadmap's language on future plans in the privacy space,[9] NIST should take great care that future activity related to privacy be tailored to implement the Framework's clearly-defined objectives, and avoid the general implementation of privacy policies which may be unrelated to assessing and responding to cyber threats. For example, Section 4.9 of the Roadmap contains discussion around developing new privacy standards beyond the Fair Information Practice Principles (FIPPS) without sufficient reference to the scope of NIST's work under E.O. 13636.[10] The executive order very clearly defines the scope of the Framework as applying to the security of critical infrastructure, and NIST's future work in the privacy space should not exceed this specified authority and go past examining the privacy implications of the activities authorized in the E.O. Should NIST undertake work on privacy issues that are outside of the scope of the Framework, it would also obscure the executive order's purpose and the work that NIST has done so far. Therefore, care should be taken so that the NIST's ongoing Privacy Engineering effort does not detract from or otherwise negatively impact the use of the Framework's existing privacy appendix.

[9] TIA's comments on the originally-proposed Framework Privacy Appendix are available at http://www.tiaonline.org/sites/default/files/pages/TIA%20Comments%20%20NIST%20Preliminary%20Cybersecurity%20Framework%20121313.pdf.

[10]

## V. CONCLUSION

TIA thanks NIST for its public request for input on awareness and initial experiences with the Framework. The ICT manufacturing and vendor community stands ready to work with NIST as it moves forward.

Respectfully submitted,

**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President & General Counsel, Government Affairs

Brian Scarpelli
Director, Government Affairs

**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**
1320 North Courthouse Rd
Ste 200
Arlington, VA 22201
(703) 907-7000

October 10, 2014