1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

February 23, 2016

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

Re: ATIS' Input to Cybersecurity Framework Request for Information

Dear Ms. Honeycutt:

The Alliance for Telecommunications Industry Solutions (ATIS) is pleased to provide input to the Request for Information (*RFI*) released December 11, 2015, by the National Institute of Standards and Technology (NIST). In this *RFI*, NIST requests information about the use of the Framework for Improving Critical Infrastructure Cybersecurity (Framework), whether there is a need to modify the Framework, and options for the long-term governance of the Framework. As noted below, ATIS members have closely examined the Framework and are utilizing key aspects of the framework in their risk analysis. Because we find that many elements of the Framework are useful, ATIS does not believe that the Framework should be modified.

About ATIS

ATIS is a technology and solutions development organization that brings together the top information and communications technologies (ICT) companies to advance the industry's most pressing business priorities, including cybersecurity, network evolution (5G, the All-IP transition, cloud services, network functions virtualization), big data analytics, emergency services, quality of service, billing support, and operations. ATIS' membership is diverse and includes stakeholders from wireline and wireless service providers, equipment manufacturers, software developers, consumer electronics companies, digital rights management companies, and internet service providers. A list of ATIS' member can be found on the ATIS website at: http://www.atis.org/membership/members.asp.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL).

One of ATIS' core missions is to foster network security and reliability, and cybersecurity is a key consideration in many ATIS initiatives. In addition, several ATIS forums are tasked with addressing cybersecurity issues, including ATIS':

- Cybersecurity Ad Hoc. ATIS' Cybersecurity Ad Hoc was launched in July 2015 to undertake a multi-step analysis of cybersecurity issues. The group is examining the existing cybersecurity Framework and has created tools to enable its effective application in risk assessment in the ICT industry. The Ad Hoc will also examine industry Best Practices that may be used to address emerging cybersecurity threats.
- Network Reliability Steering Committee (NRSC). The NRSC strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the communications industry. The NRSC addresses network reliability improvement opportunities in an open environment and advises the communications industry through the development of standards, technical requirements, technical reports, bulletins, Best Practices, and annual reports. The NRSC is comprised of industry experts with primary responsibility for examining, responding to and preventing communications outages.
- Packet Technologies and Systems Committee (PTSC). PTSC develops and recommends standards and technical reports related to packet services, architectures, and signaling, and related subjects, including next generation carrier interconnection, and signaling architecture and control. PTSC also develops and recommends implementable security standards for evolving packet-based network technologies and their interworking with other networks.

Use of Framework

In the *RFI*, NIST asks for information about respondents' interest in, and use of, the framework. As explained above, ATIS is a technology and solutions development organization representing ICT stakeholders. ATIS members companies include communications service providers and equipment providers that have closely examined the Framework and have been developing tools and practices for applying the existing Framework. ATIS members are incorporating the Framework's risk analysis methodology into a variety of business processes and uses, including internal management and communications, vendor management, and C-suite communications.

The *RFI* seeks input on organizations' experience with utilizing specific portions of the Framework (*e.g.*, Core, Profile, Implementation Tiers, Privacy Methodology). ATIS notes that its members have found the existing Framework Core to be complete and useful in the development of sound cybersecurity risk management systems for ICT ecosystems.

As to which portions of the Framework are most/least useful, it is ATIS' view that the core elements of the current Framework and the associated information references are particularly useful. ATIS believes that the implementation tiers may not be useful, particularly given that companies can garner benefits from using the Framework's risk methodology without applying the tiers.

NIST asks how to prevent duplication of, or conflict with, regulatory processes, requirements, mandatory standards, and related processes. To avoid duplication/conflict, ATIS urges NIST not to change the voluntary nature of the Framework. Mandating elements to the Framework could

have chilling effect on industry efforts to embrace the use of the Framework and to fully realize the maximum risk management benefit. In ATIS' view, industry standards, like Best Practices, must remain voluntary.

ATIS also believes that NIST's work to promote the Framework has been effective and that significant benefit has been created by NIST's ability to establish a cybersecurity risk management framework that spans multiple sectors.

Possible Framework Updates

Another focus of the *RFI* is on possible modifications or updates to the Framework. ATIS notes that its members find the Framework to be useful in addressing a broad range of cybersecurity scenarios. Consequently, ATIS does not believe that there is a need to update the current Framework. Moreover, revising the Framework at this junction could create confusion and uncertainty, and thereby potentially delay full utilization of the Framework. ATIS recommends that NIST not revise or modify the Framework.[1]

NIST seeks information regarding whether there are additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework. While ATIS is continuing its analysis of cybersecurity challenges, ATIS notes that no significant gaps or issues have been identified to the current informational references in the framework. To the contrary, ATIS believes that the current construct of the Framework, which encourages individual companies to augment the Informational References in Appendix A, is effective, and references to new/updated informational resources should be encouraged. ATIS also notes that additional best or industry best practices related to cybersecurity have been developed by industry groups such as ATIS, and in certain specific instances, private-public partnerships that the industry has with the Federal Government including NIST.

The *RFI* seeks input regarding whether there are approaches that could help other sectors or organizations if they were incorporated into the Framework. ATIS members are collaborating to develop tools and to share information on successful utilization of the Framework. ATIS believes that such work is best undertaken in sector-specific groups that can leverage members' experience and expertise in the effective application of the Framework.

NIST also seeks input on whether developments in the nine areas identified in the NIST Roadmap for Improving Critical Infrastructure Cybersecurity (Roadmap) can be used to inform any updates to the Framework. As indicated above, ATIS does not support modification to the Framework and believes that most items in the Roadmap are best dealt with via sector-specific approaches. However, ATIS notes that there are some items in the Roadmap that could benefit

[1] While ATIS does not support changes to the Framework, ATIS acknowledges that the implementation tiers may not be very useful for the communications sector. If changes are made to the Framework, ATIS would support the removal of this section.

from further examination by NIST, such as programs to increase the size of the trained cybersecurity workforce[2] and governmental alignment (both with the U.S. government and internationally) around the NIST Framework.

Sharing Information on Using the Framework

Another topic on which information is requested in the *RFI* relates to what resources have been most useful to companies in their utilization of the Framework. ATIS notes that companies in the ICT sector are making extensive use of the Framework and its associated templates. The most useful resources beyond these documents have been industry groups such as ATIS that have facilitated open dialogues among its members on cybersecurity issues and the use of the Framework.

The *RFI* also seeks information about what, if anything, is inhibiting the sharing of cybersecurity Best Practices. ATIS believes that the industry has been effective in sharing Best Practices. As ATIS noted in its comments to the Framework, significant industry work to identify and share cybersecurity Best Practices has been happening.[3] The industry database of Best Practices includes 434 industry practices related to cybersecurity. ATIS believes that the sharing and refinement of these practices in sector-specific groups such as ATIS has been effective in improving cybersecurity risk management processes. These Best Practices address recurring, or potentially recurring, challenges that have been proven through actual implementation, have been developed through rigorous deliberation and expert consensus, and have been confirmed by a broad set of stakeholders.

While the development and sharing of Best Practices is occurring, ATIS notes that concerns exist among stakeholders that NIST or another governmental agency may attempt to transform one or more Best Practices into a regulatory mandate. ATIS believes that mandating Best Practices is inappropriate for two reasons. First, Best Practices cannot be assumed to be applicable in all circumstances or to all sectors. As has been appropriately acknowledged by the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council (CSRIC), it would be impractical, if not impossible, to mandate compliance with Best Practices because not every Best Practice is appropriate for every sector of the industry, particularly as network and system designs, technologies, and capabilities differ and evolve.[4] Even within a sector, Best Practices are not "one size fits all" solutions – their use will depend on a company's business needs and deployed technologies. Second, the continued success of Best Practices in enhancing network resilience, reliability and security stems from the development of these practices in a voluntary and consensus-based environment that encourages

[2] ATIS is aware that the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council (CSRIC) is currently examining the issue of the Cybersecurity Workforce.

[3] *See* ATIS Comments to the Framework, submitted April 8, 2013 (identifying 432 cybersecurity Best Practices on the industry's database). ATIS maintains the industry's Best Practices database at http://www.atis.org/bestpractices.

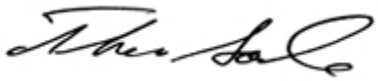
[4] Final Report of CSRIC Working Group 6: Best Practice Implementation (January 2011), Recommendation 5.2.

a pooling of vast expertise and considerable resources. The voluntary nature of Best Practices also encourages individual service providers to develop and incorporate internal standards and policies based on the Best Practices elements that are applicable, even when other elements may not be applicable. Any attempt to standardize measures, compare utilization efforts or establish compliance mandates or metrics may create a roadmap of vulnerability for cybercriminals, while at the same time producing an inflexible environment that could limit the industry's ability to respond to evolving cyber threats.

Finally, NIST seeks input on the private sector's involvement in the future governance of the Framework and on whether NIST should transition some/all of the Framework's coordination to another organization. As mentioned previously, the current Framework and NIST's management thereof is working well and should continue. Instead of transitioning this effort to another agency or private sector organization, ATIS believes that NIST should continue its lead role in the future governance of the Framework and allow industry sector-specific groups such as ATIS to continue to create tools to enable effective application of the Framework in their sectors.

If you have any questions regarding this matter or require additional information about any of ATIS' cybersecurity-related initiatives, please do not hesitate to contact the undersigned.

Sincerely,



Thomas Goode
ATIS General Counsel