From: **Tom Goode**
Date: Mon, Apr 10, 2017 at 4:14 PM
Subject: ATIS Input to Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Good Afternoon,

Attached is the ATIS input to Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity.

If you have any questions, please contact me.

Thomas E. Goode
General Counsel, ATIS

[Attachment Copied Below]

April 10, 2017

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Re: Input to Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Games:

The Alliance for Telecommunications Industry Solutions (ATIS) is pleased to provide input to the *Request for Comments* (*RFC*) released January 25, 2017, by the National Institute of Standards and Technology (NIST). In this *RFC*, NIST requests input on the changes proposed in Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity (Framework). ATIS supports the continued use of the Cybersecurity Framework as a voluntary, adaptable tool for cybersecurity risk management. However, ATIS does not support changes to the Framework to address metrics and measures or supply chain risk management.

About ATIS

ATIS is a technology and solutions development organization for the information and communications technologies (ICT) sector that advances pressing business priorities, including cybersecurity, next generation wireless and wireline network technologies (LTE, 5G, NFV), emergency services, quality of service, billing support, and operations. ATIS' membership includes stakeholders from wireline and wireless service providers, equipment manufacturers, software developers, consumer electronics companies, digital rights management companies, and internet service providers.[1] ATIS represents the ICT sector both in the U.S. and globally through its roles as the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, and member of the Inter-American Telecommunication Commission (CITEL), and as a member and contributor to the International Telecommunication Union (ITU).

ATIS works to foster network security and reliability, and several ATIS forums are tasked with addressing cybersecurity issues, including ATIS' Cybersecurity Ad Hoc. This ad hoc was launched in July 2015 to undertake a multi-step analysis of cybersecurity issues. The group is examining the existing Framework and has created tools to enable its effective application in risk assessment in the ICT industry.

---

[1] A list of ATIS' members can be found on the ATIS website at: http://www.atis.org/01_membership/members/.

Use of the Existing Framework

As an initial matter, ATIS notes that the ICT sector has been working diligently to implement the existing Framework (Version 1.0.). ATIS members have closely examined the existing Framework and have been developing associated tools and practices. 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. As many companies are still in process of implementing the existing Framework and refining their associated cybersecurity risk management processes, ATIS is concerned that introducing a new version (Version 1.1) could be disruptive to organizations' cybersecurity efforts. ATIS also questions the need for many of the new changes given previous input from many in the industry indicating that no changes were needed or desired to Version 1.0.[2]

While ATIS continues to believe that updates to the existing Framework are unnecessary, to the extent that changes are made ATIS is pleased that the application of Version 1.1, like Version 1.0, will remain voluntary.[3] Version 1.0 works well precisely because its implementation is voluntary and it does not attempt to impose a "one-size-fits-all" approach. Instead, the existing Framework is an analytical tool that helps companies determine how best to mitigate risks based on that companies specific business needs. Each company and sector of the industry can therefore use the Framework to determine how best to address cybersecurity according to its unique needs. ATIS notes that, in certain circumstances, the use of other cybersecurity frameworks or processes may be more appropriate than application of the Framework. As Version 1.1 notes, "[b]ecause each organization's risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary."[4] Therefore, ATIS supports the voluntary nature of the framework, which will allow the industry to continue to maintain the flexibility to apply a different framework and Best Practices if appropriate to manage specific cybersecurity risks.

Supply Chain Risk Management

The need for a flexible, voluntary approach is particularly important when discussing supply change risk management. Section 3.3 of Version 1.1 includes recommendations regarding the evaluation of security in the selection of a vendors' product and services.[5] ATIS notes that supply chain risk management is complex and specific procedures must be tailored to companies' unique business needs. A careful selection of only those elements of the Framework core that are important to cost-effectively manage cybersecurity risk should be used to determine

---

[2] According to NIST's Analysis of Cybersecurity Framework RFI Responses, there were "diverse" comments on whether an update is necessary or desirable, including commenters (such as ATIS) that recommended that no changes to Version 1.0 were necessary.
[3] Version 1.1, Executive Summary.
[4] Version 1.1, Section 1.0.
[5] Version 1.1, Section 3.3.

cybersecurity requirements for each specific supply chain engagement. Because there can be no standardized approach to this issue, ATIS does not think the Supply Chain related guidance in Version 1.1 is necessary. However, to the extent that this issue is addressed in the Framework, the approach taken to include Supply Chain elements as process assessment steps in Version 1.1 – identified as ID.SC-1 through ID.SC-5 in Table 3: Framework Core – may be useful in specific circumstances. ATIS also recommends that ISP Best Practices 27036 and 20243 be added to the informative references for ID.SC-1 through ID.SC-5.

ATIS is also concerned with potential unintended impacts on supply chain risk management stemming from Section 3.7 of Version 1.1. This section explains that federal agencies may find the Framework is a useful complement to existing federal risk management approaches.[6] ATIS supports efforts to encourage use of the Framework by federal agencies. However, given proposed recommendations that are being considered by Congress and the White House to require Federal agencies to use the Framework,[7] ATIS is concerned about how Federal agencies may use the Framework as part of its procurement process and whether these agencies could take an overly broad approach to the inclusion of their internal Framework profiles in procurement requirements. If an agency were to incorporate all its internal Framework profiles without appropriately tailoring these profiles to address the specific risks in a given supply situation, this could impose unnecessary costs and delays to the procurement process. If, however, supply chain risk management is addressed in the Framework, ATIS believes that more specific guidance on how to cost-effectively apply an agency's internal Framework profile to supply chain situations is needed.

Buying Decisions

Version 1.1 includes a new section explaining how the Framework could be used to inform decisions about buying products and services. ATIS notes that it will not be possible or cost- effective to impose a Framework profile as a requirement in a given procurement situation. Attempting to use a profile in this way will likely create confusion about what is actually required to meet an organization's cybersecurity specific requirements and goals. Rather, the focus should be placed on the creation and use of specific cybersecurity requirements in the procurement process. ATIS believes that it is appropriate for the Framework to recommend that such requirements be prioritized and that some sort of cost, risk trade-off analysis be performed.

Metrics and Measures

Version 1.1 includes a new section, Section 4.0, discussing cybersecurity metrics and measures.[8] ATIS believes that Version 1.1's proposed guidance regarding this issue is unnecessary for several reasons.

---

[6] Version 1.1, Section 3.7.
[7] For example, H.R. 1244, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, would foster federal agency use of the Framework if enacted.
[8] Version 1.1, Section 4.0.

First, while ATIS believes that measurement and continuous improvement are hallmarks of effective cybersecurity risk management, it notes that measuring the effectiveness of any process, including cybersecurity risk management, is highly dependent on the unique approach that a given organization uses. Efforts to standardize metrics and measures across different applications of the Framework are likely be unsuccessful as a single, standard set of metrics and measures will not address any organization's specific needs effectively.

Second, ATIS believes that the current definitions of the terms "metrics" and "measures" in Version 1.1 are ambiguous. ATIS further believes that efforts to refine the proposed definitions in any meaningful way would not be beneficial. Instead of attempting to create a standard set of metrics and measures, ATIS believes that NIST should encourage private sector organizations to select the most appropriate metrics and measures for conveying the effectiveness of their cybersecurity risk management activities.

Third, given concerns regarding the usefulness of the proposed metrics and measures in Version 1.1, ATIS believes that inclusion of this section could also frustrate efforts to encourage broader application of the Framework. The inclusion of unnecessary and potentially confusing metrics and measures may incentivize some companies to avoid implementation of the Framework.

Similarly, ATIS is also concerned that utilization of a standard set of metrics and measures in supply chain engagements will discourage the achievement of Tier 4 (Adaptive) approaches in supply chain and other Framework risk management situations. In order to operate an organization's cybersecurity risk management practices in a truly Adaptive way, the organization must be in a position to quickly adjust its target profile and the associated metrics and measures to support their cybersecurity risk management process. This will likely include metrics and measures that are not part of the Framework.

Finally, ATIS notes that the discussion of metrics and measures may be premature. Companies are still working to implement Version 1.0; adding new measurement-related provisions to the Framework will only complicate on-going implementations.

While ATIS recommends removal of Section 4.0 and the associated discussion of metrics and measures from Version 1.1, if this section remains ATIS recommends that it be replaced with a recommendation that each organization consider developing an appropriate set of metrics and measures to the extent that these are useful in the organization's unique application of the Framework.

Correlation of Metrics/Measures with Business Results

Version 1.1 of the Framework includes proposed guidance regarding the correlation of cybersecurity with business objectives in an attempt to understand and quantify cause and

effect.[9] While accountability and awareness are important, and businesses already tie risk management to business objectives, ATIS believes that it is not appropriate to map Framework core element specific *cybersecurity* practices directly to business results as suggested in Section 4.1. A subset of core elements that should be mapped in this way are already identified in the current Framework Core and ICT sector companies already routinely follow such guidance as part of larger risk management processes. For these reasons, and due to significant concerns regarding the ambiguity of metrics and measures, ATIS recommends Section 4.1 be removed.

ATIS encourages NIST to develop a national supply chain risk profile and to include this as part of the risk profile that has already been developed by NIST for the manufacturing sector. ATIS further recommends that NIST include a session during its upcoming Cybersecurity Framework Workshop, scheduled for May 16-17 on this topic.

Compliance Tool

ATIS believes that the Framework is as an excellent analytical tool for developing and improving an organization's cybersecurity risk management system. However, given the need to tailor the Framework's guidance to individual business needs, the Framework is not an effective tool for making specific decisions related to cybersecurity. Accordingly, ATIS recommends that there should be no suggestions that the Framework could be used to ensure cybersecurity risk management compliance. Confusion regarding this matter could frustrate application of the Framework by encouraging some organizations to minimize use of the Framework in favor of other, more flexible frameworks.

Conclusion

ATIS appreciates the opportunity to provide its input to the *RFC*. While ATIS supports the continued use of the Cybersecurity Framework as a voluntary tool, ATIS does not support changes to the Framework to address metrics and measures or supply chain risk management.

If there are any questions regarding this matter or additional information is required, please do not hesitate to contact the undersigned.

Sincerely,

Thomas Goode
ATIS General Counsel

---

[9] Version 1.1, Section 4.1.