Before the Department of Commerce
Washington, D.C.

In the Matter of	**)**	**Docket No. 151103999-5999-01**
Developing a Framework to Improve	**)**	
Critical Infrastructure Cybersecurity	**)**	
	)	

INTRODUCTION

AT&T Services, Inc., on behalf of itself and its affiliates (together, "AT&T") submits these comments in response to the Request for Information (the "RFI") seeking information on the "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework"). In the RFI, NIST requests information about the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance of the Framework. This information is needed in order to carry out NIST's responsibilities under the Cybersecurity Enhancement Act of 2014 and Executive Order 13636 (the "Executive Order").

AT&T commends NIST on the Framework and continues to believe that it is the best vehicle to improve the cybersecurity posture of critical infrastructure and other entities.[1] The Framework is built around the concept of risk management, which we believe provides the superior means for addressing cybersecurity, particularly given the rapidly changing nature of the threats. The Framework can be a useful tool for companies to evaluate their cybersecurity risks and build a risk management plan specific to their business. The communications sector itself has undertaken a significant effort within the FCC's Communications Security, Reliability and Interoperability Council ("CSRIC") to apply the Framework to communications critical

[1] AT&T was an active participant in the development of the NIST Framework, including participating in all of NIST's workshops, speaking on multiple panels related to the development of the Framework, and in working within the Communications Sector Coordinating Council to promote the use of the Framework throughout our industry.

infrastructure. That effort encompassed 10 subgroups and over 100 individuals from a wide variety of companies, academic institutions, non-profits and government agencies, culminating in a report that was issued in March 2015. The communications sector also has undertaken a variety of activities to promote the Framework to members of our sector, including both suppliers and smaller and midsized carriers.

As for AT&T itself, we employ a cybersecurity risk management program that predates the Framework. We currently have an internal security policy based upon widely accepted, international security standards, such as ISO 27001, PCI, SAS/70, and NIST 800-53. Many of these standards mirror the informative references included in the Framework. We use these standards to inform our internal controls that we then apply to our network systems and in protecting customer data. Thus, the Framework serves as a complement to that program. The following discusses in more detail AT&T's positions on the issues raised in the RFI.

AT&T'S SECURITY PROGRAM HAS BENEFITTED FROM USE OF THE FRAMEWORK

AT&T is one of world's largest communications companies. Operating globally under the AT&T brand, we offer one of the world's most advanced and powerful global backbone networks, provide wireless service to millions of customers with voice coverage and data roaming in hundreds of countries, are one of the world's largest providers of IP-based communications services for businesses, with an extensive portfolio of Virtual Private Network (VPN), Voice over IP (VoIP) and other offerings all backed by innovative security and customer support capabilities, and are a global leader in delivering a full portfolio of end-to-end reliable and highly secure network, voice, data and IP solutions to wholesale customers.

Given the breadth and nature of our business, it is AT&T's general corporate policy and practice to protect its information resources from unauthorized or improper use, theft, accidental or unauthorized modification, disclosure, transfer, or destruction, and to implement protective measures commensurate with their sensitivity, value, and criticality. In support of and to effectuate this policy AT&T develops and issues specific internal standards and other reference materials (the "AT&T Security Policy and Requirements" or "ASPR") that address AT&T's

workforce; its technology, vendor, contractor and supplier contracts; and overall compliance, as well as related risk-assessment practices. Given the dynamic environment in which AT&T operates, the ASPR are continually re-evaluated and modified as industry standards evolve and as circumstances require. As mentioned above, AT&T's ASPR policies are based upon industry standards, many of which are also the source of the NIST Framework's recommended standards.

AT&T's interest in the Framework is primarily as a new tool that can be leveraged to help the company, our customers, and our suppliers improve upon their existing security practices to be well positioned to mitigate large scale cyber-attacks. For example, we use the Framework to assess the comprehensiveness of our existing security policies and to determine whether there are any areas that might be enhanced through use of the Framework's standards. We also have reviewed the implementation tiers to gain a general understanding of where AT&T may fall on that spectrum.

We have found that the most useful aspect of the Framework is the implementation guidance, which contemplates a risk management process. Cybersecurity by its nature does not lend itself to a prescriptive, regulatory standards-based regime. To the contrary, prescriptive approaches are likely to be counter-productive, as they may lead users to adopt a static "lowest common denominator" methodology for dealing with the dynamic cyber threat ecosystem. In our view, regulators should take measures to streamline any existing regulations as an incentive for companies to migrate toward the Framework's risk management approach. Also, regulators should not create new regulations that will quickly become outdated and do little to prevent attacks.

THE FRAMEWORK DOES NOT REQUIRE REVISION OR "UPDATING" AT THIS TIME

AT&T does not believe it is worthwhile to pursue any changes to the Framework at this time. In our estimation, there are still many entities that are not familiar with the Framework. Companies are still trying to determine the value of the Framework in their cybersecurity practices, and any effort to revise the Framework is likely to raise additional questions that may create confusion

and negatively affect use of the Framework. Accordingly, instead of spending resources in a process of "updating" the existing Framework, NIST's objectives for cybersecurity would be best served by continuing to promote the use of the Framework, such as by providing examples of how the Framework is being applied to demonstrate its utility to industry. That in turn may help expand use of the Framework by demonstrating its business value. NIST also should to consider potential incentives and other market-based measures to drive further use of the Framework.[2]

NIST also should take steps to apply the Framework to a variety of issues related to the Internet of Things ("IoT") that have arisen since its publication. AT&T is seeing more and more IoT verticals introduced in the marketplace. Given this dynamic, there would appear to be value in NIST focusing efforts on developing use cases or examples of how the existing Framework can be used or applied in the various IoT environments.

SHARING INFORMATION ON USE OF THE FRAMEWORK

The RFI raises several questions regarding the work NIST has conducted with industry and on the sharing of best practices. In our view, NIST has been very helpful in working with industry and answering questions about the use of the Framework, including participating in the FCC CSRIC Working Groups, which as a result has helped the communications industry determine how to best use the Framework. The Communications industry has been sharing best practices for many years, both in venues established under the FCC's CSRIC, which has developed cybersecurity best practices dating back to 2003, and in a large variety of industry standards

[2] Although AT&T is convinced no update or revision to the Framework is warranted at this time, if NIST nevertheless elects to consider a change it should not be to the substantive, risk management approach embodied in the Framework. At best, there may be some usefulness to updating the Framework's references to cybersecurity standards, guidelines, and practices. Our understanding is that the Informative References in the Framework were not intended to be all encompassing, but rather to only provide examples of standards companies could use in implementing the Framework. Thus, it could be worthwhile to conduct a review of those references to ensure that they capture the majority of existing standards and possibly to update them to incorporate new standards groups, such as those we see emerging around IoT standards.

bodies, such as ATIS, GSMP, and 3GPP. Thus, in our view, the sharing of best practices on the use of the Framework and on security best practices in general is ongoing.

Nevertheless, as noted previously, NIST, and for that matter other federal agencies, could drive additional use of the Framework and best practices by providing more real world examples of the application and use of the Framework, demonstrating the business value proposition of the framework and developing incentives for its use. Just as importantly, the government can best promote cyber best practices by avoiding prescriptive regulatory regimes.

PRIVATE SECTOR INVOLVEMENT IN GOVERNANCE

The private sector should continue to drive the development of the Framework similar to the process that took place in the initial development efforts coordinated by NIST. However, NIST should carefully consider its options before transitioning some or even all of the Framework's coordination to another organization. In our experience -- in particular, as exemplified by previous activities such as the Industry Botnet Group -- it is challenging to bring an entire industry together across sectors without having some trusted entity that is not beholden to particular interests providing an overall governance role. That is what NIST accomplished with the Framework, and it is a role that NIST is well situated to continue to perform.

CONCLUSION

The RFI concludes with questions on what are the most important things that industry and NIST can do to advance the framework consistent with the objectives expressed in the Executive Order. In our view there are three fundamental steps NIST can take to reach these goals: (1) Continue to promote use of the Framework; (2) Provide use cases demonstrating how the Framework is being used; and (3) Take the existing Framework and apply it to new environments, and in particular IoT verticals, to raise the bar for cybersecurity.