Before the Department of Commerce
Washington, D.C.

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

COMMENTS OF
UNITED STATES TELECOM ASSOCIATION

The United States Telecom Association (USTelecom)[1] is pleased to submit these comments to the National Institute of Standards and Technology (NIST) in response to a Request for Information (RFI) seeking information on the “Framework for Improving Critical Infrastructure Security” (the Framework)[2]. In its RFI, NIST inquires about various aspects of the Framework since its release in February 2014,[3] with particular interest on ways in which it 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.”

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets.

[2] See, Federal Register Notice, Department of Commerce, National Institute of Standards and Technology, Request for Information, *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, 80 FR 76934 (December 11, 2015) (available at: https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity) (visited February 16, 2016) (*NIST RFI*).

[3] See, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, (released February 12, 2014) (available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

USTelecom notes that based on numerous observations and experiences, the Framework has had a profound impact on our nation's progress in addressing cybersecurity concerns. Most notably, in the roughly two years since its release, the Framework has become a foundational cornerstone of public and private sector discourse by providing internal enterprise and external stakeholders with a common language to describe and implement cybersecurity risk management programs. Conversations about cybersecurity risk management generally, and the Framework in particular, are now commonplace within many organizations. As one USTelecom member recently remarked, "cybersecurity is not just an IT issue, it is a business issue of critical strategic importance." Equally significant is the dialogue that has ensued between industry sectors and their government partners who must work in unison to ensure that the core principles articulated in the 2013 Executive Order[4] and embedded in the Framework are achieved.

A. The Communications Sector Has Fully Embraced the Framework

The communications sector has played a noteworthy role in both the development of the Framework and its evolution since its issuance. Working through sector trade associations and the Communications Sector Coordinating Council (CSCC), our industry participated in all of the NIST workshops and subsequent discussions and helped to ensure that the final product would be embraced by member companies based on its self-evident value. At the time of the release, AT&T CEO Randall Stephenson appearing at a White House event to mark the occasion stated unequivocally that his organization would use the framework as a basis for evaluating risk,

[4] Executive Order, *Improving Critical Infrastructure Cybersecurity*, (released February 12, 2013) (available at: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) (visited February 16, 2016).

especially with regard to managing vendor relations[5]. Other companies followed suit even as the sector prepared for a major undertaking to advance alignment with the NIST framework.

Working with the Federal Communications Commission's (FCC) Communication Security Reliability and Interoperability Council (CSRIC), the industry embarked on a year-long study to adapt the sector-agnostic Framework to the five segments that comprise the sector which include broadcast, cable, satellite, wireless and wireline companies. Over 100 participants representing a wide array of companies (including international corporations), academic institutions, non-profits, and government agencies produced a Final Report that companies of all sizes can use to apply the Framework within their environments in a prioritized, cost-effective and flexible fashion.[6] Moreover, consistent with recommendations that were included in the study, the sector has contributed to the voluntary C-cubed program under DHS[7], conducted numerous independent outreach events,[8] and is currently incorporating cyber threat evaluations

[5] Aamer Madhani, USA Today, *Obama administration unveils cybersecurity guidelines,* (February 12, 2014) (available at: http://www.usatoday.com/story/news/politics/2014/02/12/white-house-cybersecurity-framework-released/5422129/#) (visited February 16, 2016).

[6] The Communications Security, Reliability and Interoperability Council IV, Final Report, *Working Group 4: Cybersecurity Risk Management and Best Practices*, March 2015 (available at: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf) (visited February 16, 2016).

[7] See, Department of Homeland Security website, *Critical Infrastructure Cyber Community C³ Voluntary Program*. (The C³ Voluntary Program is designed to assist stakeholders with understanding use of the Framework and other cyber risk management efforts, and support development of general and sector-specific guidance for Framework implementation, available at: http://www.dhs.gov/ccubedvp) (visited February 16, 2016)

[8] *See e.g.*, USTelecom webinar, *Telecom Cyber Frameworks, Policies and Business Processes*, May 28, 2015, (available at: http://www.ustelecom.org/events-education/webinars/telecom-cyber-frameworks-policies-and-business-processes) (visited February 16, 2016); *see also*, USTelecom webinar, Telecom Cyber Risk Management, Operational & Technology Requirements, June 18, 2015 (available at: http://www.ustelecom.org/events-education/webinars/telecom-cyber-risk-management-operational-technology-requirements) (visited February 16, 2016); *see also*, USTelecom webinar, Cyber Risk Management,

into the CSCC's 2016 Sector Annual Report. All of these industry efforts, within and across sectors, speak to the considerable influence the Framework is having in shaping cybersecurity activities across a broad landscape.

B. The USTelecom Member Survey Captures Important Perspectives on the Framework

To provide NIST with the feedback it is looking for and to address questions about potential future efforts to advance the Framework, USTelecom conducted a survey of its members that explored questions raised by NIST and conducted additional in-depth one-on-one discussions with member companies. While individual companies have unique needs, interests, and approaches, we were able to capture some important perspectives that could help inform future activities.

1. Companies are Using the Framework in Diverse and Innovative Ways

Companies are finding innovative and flexible ways to use the Framework that are often tailored to address very specific interests and circumstances within the organization. The flexible structure and architecture of the Framework allows companies to extract elements that they deem to have the highest potential value for their enterprise. The fact that it is not a rigid checklist and encourages companies to evaluate informative references (both identified and non-identified), allows companies to tailor and scale systems and processes consistent with their risk tolerance and resource constraints.

Operational & Technology Requirements Continued, July 23, 2015 (available at: http://www.ustelecom.org/events-education/webinars/cyber-risk-management-operational-technology-requirements-continued) (visited February 16, 2016).

For example, one member commented on how the Framework effort led them to find value and embrace another government initiative. They claimed that “the Framework concept of target profiles and the underlying notion of continual review and improvement of cyber risk management policies and procedures have led us to embrace the Department of Homeland Security’s Cyber Resilience Review as a method of assessment. We are on our second round of meetings since the Framework was released, and it has allowed us to focus on which core functions and activities best balance advancing our cyber risk management maturity with what makes the most business sense.” Another member commented that “we use the Framework for internal security management across our business divisions and it is central to messaging to business leadership.” Another company noted that “the Framework has become an integral part of our cybersecurity risk management program and that it was very effective in communicating the objectives of cybersecurity programs to our management team.”

A significant finding from our survey went to the question of the Framework’s impact on member companies. In characterizing the extent that our members believe the Framework has helped reduce their cybersecurity risk, half of the respondents indicated that they can point to “some success” and half indicated that there had been “substantial success.” None of the respondents answered “none” or “little.” With less than two-years since its inception, these promising results speak to the substantial impact that the Framework is already having on industry.

2. Companies are Integrating the Framework into the Flexible Manner That Was Intended

Member companies are pointing to different components of the Framework they find useful and that they have incorporated into their existing cyber risk mitigation programs. One company indicated that they are only using the “Core” and that they have “no current plans around profiles or tiers" while another company remarked that "the core and target profile guidance has assisted in developing and communicating cybersecurity posture." Overall, the general sense from respondents is that the tiers are difficult to apply, because assigning values based on the descriptions is challenging and akin to what one member characterized as "an exercise in excessive contemplation." Another member noted that the "implementation tiers as described do not translate directly to executive boards…" and that "it would not be immediately understandable to the Board to say the program is Tier 3 and Repeatable. CISOs understand the concept and will just need to translate as appropriate." It is also apparent that many companies are assessing their risk posture based on both the category and sub-category level. One company stated that the Framework Core was most useful because of the "easy linkage to the essential NIST 800-53 controls as referenced."

3. **The Framework Should Remain a Voluntary Construct and Free From Regulation**

Not surprisingly, this issue was one that received considerable attention and uniform agreement among our members. The notion that the Framework remains voluntary and not be "coopted" into a regulatory compliance regime is widely held across the membership. Members praise the approach taken by our federal regulator, the FCC, in working in partnership with industry to preserve the voluntary and flexible nature of the Framework, and at the same time promoting the use of a risk management approach that the Framework embodies.

Expressing a sentiment shared by many members was the comment that "any prescriptive approach to cybersecurity would be counter-productive and would only produce a false sense of security. The environment we face today is one in which the bad guys want nothing more than for companies to follow a rigid playbook. We have seen our adversaries adjust tactics measured in hours and what were advanced threats yesterday have become run-of-the-mill threats today.

This is one area that requires constant innovation and experimentation and government must recognize that 20th century regulatory models will not protect us."

We also note our appreciation to NIST for their outreach efforts to state and local government officials including workshops and meetings with state agencies and participation in various NARUC events. We believe it is imperative for state regulatory commissions to avoid duplicative or inefficient activities, and we encourage NARUC and the states to work with our government partners and industry to find rational and productive avenues for engagement. We also maintain that the voluntary approach embodied in the NIST Framework will benefit the states in managing their cybersecurity risk and we are encouraged to see that many states have already adopted the Framework as a basis for protecting their critical networks and systems.[9]

We strongly urge NIST to continue to facilitate a sustained dialogue between regulators and industry and to explore approaches that lead to mutually beneficial results.

4. NIST Should Continue to Guide Near-Term Framework Development Efforts

USTelecom members urge NIST to continue to play a key role in facilitating further Framework development activities. Given the competence demonstrated throughout the effort and the proven ability to bring a broad array of stakeholders to the table, it would be premature at this time to transfer responsibilities to the private sector. Continued engagement not only ensures that further progress will be made, but also is consistent with the set of statutory

[9] *See*, NIST website, *State and Local Government Cybersecurity Framework Kickoff* (available at: http://www.nist.gov/itl/state-local-govt-cyber-framework-kickoff.cfm) (visited February 16, 2016).

responsibilities set forth in the Cybersecurity Act of 2014[10]. Moreover, some policy makers will continue to debate the value and effectiveness of the Framework and NIST is a vital advocate for continuing on a path that has demonstrable success and great promise going forward. One member offered a widely shared view stating that "NIST should continue to be the 'convener and coordinator' of the [Framework] for the foreseeable future. Having this function move out of the government would embolden other agencies to compete to become the 'authoritative' voice of cybersecurity in the government and perhaps guide future versions of the Framework towards a more prescriptive approach."

5. <u>Any Update of the Framework should be Incremental and Focus on Consensus-based Gaps</u>

The general sense among USTelecom members is that a Framework "overhaul" that is too broad in scope could have a disruptive effect on current enterprise integration efforts. However, USTelecom members do not view the Framework as a static instrument and wish to see it evolve in ways that enhance its usability and effectiveness. It is certainly not necessary to convene the type of effort that was required to develop Version 1.0 with all of the attendant workshops. As one of the RFI questions infers, the key is to "minimize or prevent disruption for those currently using the Framework."[11] One member echoed this sentiment stating that consistency with the current Framework should be maintained and that "keeping the Framework's risk-based approach will minimize disruption as organizations only adopt what makes business sense." Speaking to a broad industry concern about priorities, one member noted

[10] National Cybersecurity Protection Act of 2014, S.2519 (available at: https://www.congress.gov/bill/113th-congress/senate-bill/2519/text?q=%7B%22search%22%3A%5B%22s.2519%22%5D%7D) (visited February 16, 2016).

[11] *NIST RFI*, question 24, p. 76936.

that “NIST should focus on risk management approaches that have the most bang for the buck and have broad support across industry and government.”

6. NIST Can Facilitate Further Sharing of Framework Information

The future success of the Framework will depend in large part on the extent to which individual enterprises share their experiences and learn from the experience of others. NIST can play an important role in developing a structured program and repository to capture information on a wide array of Framework implementation considerations, including among other things, guidance on approaches to cost-benefit analyses, internal and external stakeholder communications, updated technical informative references and their applicability to the Framework, use of the core, profile and tier constructs, regulatory alignment, and innovative uses of the Framework. One member noted that “NIST can be very effective in distributing information to Framework users since security-related benefits are often limited to informal word-of-mouth processes.”

7. Work Should Continue to Promote International Alignment

The global nature of cybersecurity risk calls for an approach that transcends national boundaries. The NIST Framework has already influenced risk management activities and discussions among domestic enterprises. Many of these companies have global operations and disparate regimes create confusion and inefficiencies. NIST has been active in visiting other nations to explain why and how the Framework was developed and how it is being used by organizations. NIST should continue to facilitate international recognition of the voluntary Framework as a model for global cybersecurity risk management activity.

In this upcoming phase, NIST should evaluate what has been accomplished at the international level and how best to build upon some early success.

C. Conclusion

We applaud NIST for undertaking this timely review of the Framework and to seek input from those most impacted by its use. As NIST contemplates additional work in this area, USTelecom and it members stand ready to engage in a productive multi-stakeholder collaborative effort.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: Robert L. Mayer

Robert Mayer
Kevin Rupy

Its Attorneys

607 14th Street, NW, Suite 400
Washington, D.C. 20005
202-326-7300

February 17, 2016