Before the Department of Commerce
Washington, D.C.

In the Matter of	**)**	
	)	
Experience With the Framework for	**)**	**Docket No. 140721609-4609-01**
Improving Critical Infrastructure	**)**	
Cybersecurity	**)**	

COMMENTS OF THE US TELECOM ASSOCIATION

US Telecom Association
607 14th Street, NW
Suite 400
Washington, DC 20005
(202) 326-7300

Jon Banks
Senior Vice President, Law and Policy

Robert Mayer
Vice-President, Industry and State Affairs

October 10, 2014

TABLE OF CONTENTS

I. INTRODUCTION

The US Telecom Association ("USTelecom") submits comments in response to the Request for Information ("RFI")[1] from the National Institute of Standards and Technology ("NIST") regarding the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework").[2] USTelecom and its members have actively participated in policy and technical discussions about cybersecurity and the Framework, and we welcome the opportunity to share our perspectives on awareness, experiences, and ideas for the future of the Framework. First, NIST asks a series of questions to elicit feedback about awareness of the Framework and its key attributes. NIST next inquires about the private sector's early experiences with the Framework. Finally, NIST solicits feedback on its *Roadmap for the Future of the Cybersecurity Framework*.[3]

USTelecom represents broadband service providers and suppliers for the telecom industry. Our diverse membership ranges from large publicly-traded communications corporations to small private cooperatives—all providing advanced communications services to urban and rural markets. As the Internet becomes more widely available globally, cyber attacks have increased. USTelecom's members play an important role in this diverse and interconnected ecosystem. We have a Cybersecurity Working Group, including legal, technical, and policy representatives from member companies that collaborate to identify tools to enhance cybersecurity. We are pleased to provide NIST with early feedback on the Framework.

II. CURRENT AWARENESS OF THE CYBERSECURITY FRAMEWORK IN THE COMMUNICATIONS SECTOR.

Awareness of the Framework among large and small USTelecom members is substantial. The Framework has become a common discussion point for advancing cybersecurity risk management activities. Many of USTelecom's member firms already implement methodologies in the Framework and are now evaluating or using it to supplement existing practices. And even though our smaller members in most instances do not meet the threshold "critical infrastructure" designation,[4] they recognize the importance of cybersecurity and have begun efforts to implement the Framework's ideas. NIST's efforts are reaching their intended audience in the communications sector.

USTelecom members learn about the Framework through a variety of venues, as expected. Many members were active participants in the development process, including NIST-sponsored workshops. This significant level of engagement provided our members with a unique

---

[1] NIST, *Experience with the Framework for Improving Critical Infrastructure Cybersecurity*, Request for Information (Aug. 26, 2014), *available at* https://www.federalregister.gov/articles/2014/08/26/2014-20315/experience-with-the-framework-for-improving-critical-infrastructure-cybersecurity.

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[3] NIST, *Roadmap for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf ("*Roadmap*"). The *Roadmap* accompanied the Framework in February 2013.

[4] Executive Order No. 13,636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

opportunity to influence the substance of the Framework, and it gave them a deep understanding of how they could choose to use the Framework to achieve enterprise-specific objectives. Further, many of our members continue to contribute to the growing awareness through ongoing involvement in sector and cross-sector efforts to refine risk management practices. Members are learning about the Framework through a variety of industry and government activities, including:

- the Department of Homeland Security ("DHS") Critical Infrastructure Cyber Community C³ ("C³");[5]
- outreach work conducted through the Communications Sector Coordination Council ("CSCC");[6]
- the current Federal Communications Commission ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC") IV Working Group 4 effort;[7] and
- media and trade reports.

Members also learn and share information about the Framework through USTelecom outreach. USTelecom actively engages members to keep them abreast of ongoing developments across industry and government. We have recently created a new USTelecom small/mid-size company cybersecurity working group to enhance members' awareness and to address resource issues and constraints that present unique challenges for companies with scale limitations.

USTelecom engages in outreach to spread awareness not just to our members, but to the broader communications sector as well. We advance outreach efforts through engagement with the CSCC, which has sponsored webinars with DHS, including one planned for late October to present and describe the work being undertaken in CSRIC IV Working Group 4. Our members are active participants in many workshops and meetings to promote the Framework, and we will continue to support outreach activities in multiple public-private partnership venues. What is more, the Framework development process and subsequent outreach efforts have spurred members to be more proactive with internal communications as a deeper awareness of the Framework gains traction within the enterprise.

USTelecom and our members are actively engaging with other organizations to further our understanding of the Framework and to share lessons learned about it and other security issues. Indeed, the sharing of ideas and learning from the work of others is a long-standing concept engraved within our members' security practices. Specifically, relevant to the Framework context, our members primarily work through the CSCC to share information, and many also are active in the Comm-ISAC,[8] the FCC's CSRIC and Technological Advisory

[5] The C³ Voluntary Program intends to "be the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The C³ Voluntary Program aims to: 1) support industry in increasing its cyber resilience; 2) increase awareness and use of the Framework; and 3) encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management." *See* http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program.

[6] *See* http://www.commscc.org/.

[7] *See* http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv.

[8] *See* http://www.dhs.gov/national-coordinating-center-communications.

Council ("TAC"),[9] the President's National Security Telecommunications Advisory Committee ("NSTAC"),[10] and several non-profit associations.

NIST prudently inquires about activities and awareness in other parts of the federal government. The FCC is well aware of the Framework and has supported it as a core element of enhancing cybersecurity risk management practices within the communications industry. The FCC is advancing the evolution of the Framework through its CSRIC, which has a longstanding role in developing voluntary practices and encouraging their use where appropriate. There are currently over 100 individuals representing the broadcast, cable, wireless, wireline, and satellite segments, as well as other stakeholders, working to adapt the Framework to each segment through the CSRIC IV Working Group 4, which USTelecom co-chairs with TimeWarnerCable.[11] This effort is designed to align closely with Framework constructs and principles. Like the Framework process at NIST, CSRIC's mission is to offer solutions that are voluntary, flexible, and capable of being tailored to individual enterprises. It includes NIST in a key advisory role. A final report from Working Group 4 is expected to be presented in March 2015 and will include recommendations to the FCC to utilize the Framework as a central element of future cybersecurity coordination and collaboration among diverse stakeholders throughout the ecosystem. As with NIST's efforts, the CSRIC is an organization of volunteers with output that includes voluntary recommendations—not regulatory mandates. It is important that CSRIC retain its core, voluntary mission and approach.

USTelecom's ongoing work to support the Framework provides members a comprehensive appreciation of its goals and structure. For example, USTelecom members are keenly aware that the Framework is intended for voluntary use—this message is often reinforced by government and industry officials. The Framework must remain truly voluntary to be effective. Cybersecurity mandates to adopt or periodically report on practices should be avoided, as mandates could cause some organizations to only "meet the standard" and not develop independent initiatives to address evolving threats.

USTelecom's members understand that the Framework is a cyber risk management tool for all levels of an organization and that it builds on existing cybersecurity tools. *First*, the Framework is useful for companies as they consider the appropriate mix of cybersecurity practices. While the Framework might not provide new information for companies that already have sophisticated practices, it might be very useful for other companies. As the Framework was released just nine months ago, USTelecom expects that it will take time for an enterprise to evaluate how it fits into the enterprise's overall risk management approach before the cybersecurity component can be effectively communicated to all levels of the organization and to third-party stakeholders. *Second*, many members are aware that the basis for the Framework comes from existing cybersecurity standards. However, some organizations may be unfamiliar

[9] *See* http://www.fcc.gov/encyclopedia/technological-advisory-council.

[10] *See* http://www.dhs.gov/nstac.

[11] CSRIC's Working Group 4 set out to "evaluate CSRIC's most critical existing cybersecurity best practices and determine how best to improve them to account for changes in cybersecurity practice and the threat landscape. The Working Group will also harmonize these best practices with the recently released NIST Cybersecurity Framework. In addition, the working group will explore aspects of a business environment in which cybersecurity-specific practices will be effective, efficient, and sustainable." *See* CSRIC IV Working Group Description, *available at* http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv.

with existing cybersecurity standards, guidelines, and other practices. A major benefit of the Framework is that it points companies to important, informative references as they enhance their cybersecurity risk management postures.

As NIST recognizes, there are some challenges to improving awareness of the Framework. As a general matter, it may be challenging for some providers to keep up with continuously evolving security threats while simultaneously implementing the Framework or other cybersecurity risk management capabilities. One key challenge is the desire by some policymakers to draw immediate correlations between the use of the Framework and some objective measures of improvement in cybersecurity outcomes.[12] Efforts are ongoing to explore such indicators, but these efforts are likely to take substantial time.

Some challenges are specific to the communications sector. One challenge is that the industry is global. Industry members must adhere to the laws and regulations of countries where they have operations, while incorporating the guidance of a domestic, voluntary Framework. Another challenge is the diversity of the communications industry. Even though the sector is largely aware of the Framework, there are thousands of communications providers nationwide, and many are in rural areas. It is a challenge to reach everyone, which is why the flexibility built into the voluntary Framework is critical. Another major challenge—which is also an opportunity—is the rapidly changing technology used by the industry's customers, employees, and network equipment providers. The challenge is keeping up with technology changes and new vulnerabilities they introduce; the opportunity is the ability to leverage new technologies to increase awareness of cybersecurity issues and threats.

NIST inquires about international awareness of the Framework. It is difficult to assess the current level of international awareness but we know that other countries are aware of and looking at the Framework. Many countries appear to have adopted a wait-and-see attitude. There is genuine interest in what is happening in the United States, but it is incumbent upon the U.S. government and private sector to demonstrate the benefits of the Framework's voluntary and flexible approach. Furthermore, even though international awareness currently is difficult to assess, the U.S. government should continue its efforts internationally to promote the voluntary use of widely-adopted, consensus-based standards to address cybersecurity, as opposed to taking a checklist-approach. And it is important that the U.S. government be consistent in its approach; it should not evangelize the *voluntary* Framework abroad while at the same time advocating or threatening to pursue regulations domestically.

III. EXPERIENCES WITH THE CYBERSECURITY FRAMEWORK IN THE COMMUNICATIONS SECTOR.

The communications industry continues to be a leader in cybersecurity risk management, with a decades-long history of working with government agencies to address evolving threats to

[12] For example, the Administration recently urged industry to supply the government with input regarding metrics to assess the Framework and cybersecurity. *See White House Seeks More Industry Input on Cyber 'Metrics,'* Inside Cybersecurity (Oct. 1, 2014), *available at* http://insidecybersecurity.com/index.php?option=com_user&view=login&return=aHR0cDovL2luc2lkZWN5YmVyc2VjdXJpdHkuY29tL0N5YmVyLURhaWx5LU5ld3MvRGFpbHktTmV3cy93aGl0ZS1ob3VzZS1zZWVrcy1tb3JlLWluZHVzdHJ5LWlucHV0LW9uLWN5YmVyLW1ldHJpY3MvbWVudS1pZC0xMDc1Lmh0bWw=.

networks and customers. Members are still in the early stages of evaluating the Framework, but it appears useful to members across the spectrum of cyber-preparedness.

A. The Framework's use will depend on organizations' practices and capabilities.

Not surprisingly given varying risk profiles and customer demands, USTelecom's membership reflects a range of cybersecurity risk management capabilities. As we recently pointed out in an FCC filing, the market holds companies accountable for cybersecurity practices. For broadband service providers, the primary source of revenue depends on network integrity, functionality, and availability. Nothing could be more inextricably linked to market accountability than continuity of operations. Cybersecurity attacks and data breaches have major repercussions for companies across all industries.

In the nine months since the Framework was released, USTelecom members have had varied experiences that reflect their existing profiles. For some members, the Framework is being used to supplement and inform existing practices. For other members, the Framework may serve as a tool to consider new processes. Fundamentally, it is driving an increased focus on cybersecurity as a government priority. In some instances, the Framework has provided member companies with added support for and emphasis on purchasing and planning decisions centered on network security. For some members, increased government and public attention has resulted in increased discussion and awareness about cybersecurity at all levels of their organization. Such increased awareness and engagement shows that the Framework is helping to reinforce the importance of managing cyber risk. This constitutes early success.

Many members have highly mature cybersecurity risk management capabilities, and for those members, the Framework reinforces existing mechanisms developed over many years to enhance cybersecurity risk management endeavors. These organizations understand the importance of managing cyber risk, and have programs in place to identify, prevent, detect, respond to, and recover from cyber attacks, and their customers are increasingly aware of cyber risks. As well, many of these companies have pointed to the Framework as a useful tool when determining how to best defend against cyber threats. Many USTelecom members have already been using industry practices and international standards in the Framework to assist with cyber risk management. Indeed, for some members, existing cyber risk management methods could be thought of as a super-set of practices and principles that include aspects of the Framework, and for these companies, their methods are even more comprehensive than the Framework's. For member companies serving sophisticated and demanding enterprise customers, expectations are that the service provider offerings conform with standards specific to their sector. By contrast, for members that are building capabilities, the Framework can be an important foundation to communicate the risk profile to upper management to obtain the resources that are required to meet targeted security objectives.

B. The sector is reviewing how the Framework complements existing practices.

The Framework remains in its early stages, and as such, most members are still evaluating and determining how best to use it. That hard work is underway in CSRIC and elsewhere. While that continues, USTelecom can share with NIST some observations based on early experiences.

Regardless of the level of security sophistication, most member companies that are aware of the Framework are reviewing how it can complement their programs. NIST asks about its use in enterprise risk management. In almost all instances, integration with broader enterprise risk management programs is still in the planning and review stages. Many members are assessing how to use the Framework's recommended practices, especially in light of the fact that many of the recommendations—including identifying an organization's core mission, the threats to that mission, the current and desired state of security, and a roadmap to get to the desired state of security—are basic risk management practices that most cyber-risk aware companies within the communications sector already follow. USTelecom's members continuously improve their security practices and adapt them to changing technologies, customer expectations, and emerging threats. Members are currently assessing how the Framework can help inform and guide these practices on a going-forward basis. Some members do not anticipate significant changes to their risk management approaches as a result of the Framework. Others indicate they may use it to update their processes for cybersecurity. Likewise, many members employ their own privacy measures and are still evaluating the privacy and civil liberties portions of the Framework.

NIST inquires about the need for sector-specific guidance. Although many members will not need additional guidance to use the Framework, a subset of providers may require additional resources and guidance to move forward with implementation. To that end, the communications sector is working on developing this analysis and guidance as part of CSRIC IV Working Group 4. That effort includes a separate evaluation of the Framework and related guidance for small and mid-sized companies. The CSRIC Working Group 4 also has a separate effort underway to consider barriers and challenges to using the Framework and will be developing use case studies to determine how providers have or might overcome such obstacles. As discussed above, USTelecom members are participating in this NIST adaptation work. That project will provide important insights into how individual companies can evaluate their own voluntary use of the Framework. This project has a segment-specific focus, an approach that is consistent with the Framework's recognition that organizations, sectors, and industries have different risk profiles, capabilities, and operational constraints. This flexibility is consistent with NIST's iterative process and will help to ensure that the use of the Framework takes into consideration aspects unique to the communications sector.

As companies experiment with the Framework, a more complete picture of its benefits will emerge. Some early benefits have become apparent. Many members recognize the value of having a common taxonomy, as provided by the Framework, to communicate across internal organizations and with other organizations that provide services and products that they are dependent upon.[13] Indeed, for some members with highly mature capabilities, a major benefit of the Framework has been that it provides a common reference guide of standards and other practices. The Framework's use of core, profile, and implementation tiers provides a good basis for an organization to begin discussing how best to update its cybersecurity risk management

[13] Even though members recognize this benefit, many are still considering whether to use the Framework to communicate information about cybersecurity risk management programs to stakeholders, and whether to use the Framework to express cybersecurity requirements to partners, suppliers, and other third parties. While members routinely communicate information about cyber risk management to various stakeholders, to our knowledge, none are yet using the Framework specifically as a vehicle for those communications. Members' communication of cybersecurity requirements to partners, suppliers, and other third parties differs depending on the organization.

maturity posture, although it would be beneficial to have further clarification of the current tier criteria.

Perhaps the most helpful aspect of the Framework is that it is designed to be flexible and to allow organizations to tailor it for their unique risk considerations. The Framework is not designed to be a one-size-fits-all program or the basis for a checklist compliance regime. Instead, it offers a logical approach to cyber risk management. For organizations that lack a comprehensive cyber risk management plan or desire to learn more about the process, the voluntary Framework is an excellent starting point. USTelecom is working closely with its members to ensure that Framework efforts are proceeding at an appropriate pace, and we recognize that each organization will face distinct challenges and must be given time to identify and address them.

Because industry is still assessing how the Framework relates to particular sectors and to individual organizations' practices and postures, USTelecom cautions against any sort of rigid timeline or expectations regarding the pace of implementation and the type of use. Doing so, in the absence of a proper foundation, could undermine the efficacy of the Framework and the collaborative process underway at NIST and elsewhere.

C. NIST and other agencies can promote a broader approach to the Framework.

NIST's development of the Framework confirms the unique role that government can play in facilitating broad industry engagement. To further promote implementation of the voluntary Framework, USTelecom urges the National Telecommunications and Information administration ("NTIA") to initiate an Internet Security Task Force that follows-up on its June 2011 Green Paper.[14] A renewed look at these issues in an NTIA-led process can include more stakeholders than any one agency can convene. And it can use the Framework as a starting point. This effort will increase awareness that effective cybersecurity must address threats, vulnerabilities, and innovative solutions across a broad ecosystem.

This broader effort is needed because issues involving Internet security, such as DNS, BGP, mobile, the Internet of Things, and cloud computing, require collaboration across the global ecosystem. NTIA can play an important convening role to organize activities, while still allowing industry to develop common practices or recommended solutions. The U.S. government should avoid fragmented agency initiatives in this space, and participants across the government should participate in a multi-sector Internet security initiative. With the NTIA and the Department of Commerce acting as convener, as opposed to there being a sector-specific convener, a broader set of stakeholders would be brought to the table. This would result in industry being able to develop more effective solutions.

USTelecom also recommends that more attention be given to smaller organizations that may not have the resources available to evaluate and implement the Framework. Many federal agencies could help with this effort, including the Small Business Administration. As other opportunities arise, agencies should be inclined to assist small business with these efforts.

[14] Department of Commerce Internet Policy Task Force, *Cybersecurity, Innovation and the Internet Economy* (June 2011), *available at* http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

IV. ROADMAP FOR THE FUTURE OF THE FRAMEWORK IN THE COMMUNICATIONS SECTOR.

USTelecom agrees with NIST that the areas identified in the *Roadmap* are appropriate to consider in future activities related to the Framework. In the key areas that NIST identified in its *Roadmap*, we are not aware of any major development work underway that has not been brought to the attention of NIST and other stakeholders. From the perspective of the communications sector, USTelecom believes that in addition to the areas identified, future engagement should consider how to foster a consistent and predictable environment for innovation and research and development around cybersecurity.

Fostering innovation is important because cybersecurity efforts cannot stand still. We cannot rely on a snapshot of identified threats, best practices, or standards. This is why regulation or assurances based on existing practices would be misplaced. To the extent the Executive Order and the Framework are predicated on previously-identified risks and widely-accepted common standards, even their laudable voluntary approaches risk almost immediate obsolescence. This is a general weakness of reliance on standards, which fosters a backwards-looking approach that allows cyber attacks to circumvent static protections. A process that catalogs and measures compliance with standards or approaches already developed and in use does not lend itself to exploring new solutions that may prove more adept at staying in front of ever-changing cyber attacks. The market already demands innovation, but to the extent that government seeks to supplement market-driven incentives and solutions, USTelecom urges NIST and the government generally to avoid placing too much reliance on existing standards and approaches. USTelecom recommends that in the area of incentives, NIST initiate and facilitate discussion about research and development for cybersecurity. It can examine how government can play an effective role in fostering innovation in the cybersecurity arena, similar to the work being done with the National Cybersecurity Center of Excellence.

USTelecom also urges NIST to consider how it can foster harmonization and avoid balkanization. Most major U.S. companies have significant operations or stakeholder dependencies worldwide, so NIST should work with industry to advocate for other countries to adopt a similar voluntary approach to cybersecurity risk management. Domestically, USTelecom is concerned about divergent approaches among federal agencies, but also at the state level, which could divert energy from effective partnerships and progress underway. We encourage NIST to heed efforts by states in cybersecurity. The federal government should work to promote a unified national approach to avoid balkanization of efforts and standards and the inefficient allocation of scarce technical resources.

V. CONCLUSION

USTelecom applauds the Framework. A substantial number of our members are aware of the Framework and its key points—in particular, its voluntary nature. While experiences vary from member to member, USTelecom appreciates that the Framework is flexible and intended to evolve with use and innovation. The Framework is new. Over time, its benefits can be fully assessed and its approach refined. In future versions, USTelecom urges NIST to focus on innovation and research and development to stay ahead of ever-evolving cyber threats.