January 19, 2018

Via cyberframework@nist.gov

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

Re: Cybersecurity Framework Version 1.1 Draft 2

Dear Mr. Games:

USTelecom[1] appreciates this opportunity to comment on Draft 2 of Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity ("Draft 2"), released by the National Institute of Standards and Technology ("NIST") on December 5, 2017.[2] In short, Draft 2 of the Framework reflects a substantial improvement over the initial Version 1.1 on which NIST sought comment a year ago, particularly with respect to the important and still-developing discipline of cybersecurity measurement. While Draft 2 of Version 1.1 addresses for the first time other important cybersecurity challenges such as supply chain risk management and coordinated vulnerability disclosure, this submission places its primary focus on cybersecurity measurement. Applying this maturing discipline to an organization's self-assessment of cybersecurity risk and risk management is at the heart of individual organizations' efforts to develop effective, customized methods to conduct cybersecurity risk management.

Overview and Context

As the Framework approaches the end of its fourth year of implementation following the publication of Version 1.0 in February 2014, USTelecom and its U.S. and international members will endeavor to promote the use of Framework Version 1.1 and accelerate its implementation as an advanced risk management tool in order to build cybersecurity resiliency throughout the global internet and communications ecosystem. In 2014 and 2015, we helped lead the groundbreaking initiative under the fourth Communications Security, Reliability and Interoperability Council ("CSRIC") to develop tailored Framework implementation plans for each of the five segments of communications sector (wireless, wireline, cable, satellite, and broadcast). This CSRIC initiative was, and remains, the most ambitious and in-depth

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks.

[2] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 Draft 2 (rel. Dec. 5, 2017), *available at* www.nist.gov/cybersecurity-framework ("Latest Updates").

Framework implementation effort in any segment of the economy. We know very well that use and implementation of the Framework requires disciplined analysis and rigorous corporate governance.

With that in mind, USTelecom proposes to work with NIST and other partners to build on those previous efforts through, among other initiatives, the collection of successful "use cases" of Framework implementation by organizations worldwide. Because cybersecurity threats are global in nature, our shared learning about them should be as well. Collecting and promoting examples of dynamic, innovative improvements in Framework implementation – including cybersecurity measurement for organizations' self-assessment of risk – from a diverse array of domestic and international sources can help advance this implementation in all facets of Framework risk management.

Cybersecurity Measurement and Self-Assessment of Risk

Last April, in response to the first proposed Version 1.1 of the Framework, USTelecom recommended that NIST should pursue a collaborative approach to further development of the Framework and avoid any actions that could move it in the direction of a compliance regime with prescriptive standards leading to private sector audits and reporting. To that end, USTelecom urged caution in connection with the use of metrics to evaluate the Framework's effectiveness in reducing cybersecurity risk, emphasizing that it is important for NIST and the private sector writ large to develop a measurement approach that can be used as a reliable indicator of our nation's progress in using risk management processes to improve critical infrastructure cybersecurity. USTelecom observed, however, that the approach to measurement taken in the first iteration of Framework Version 1.1 risked departing from these fundamental principles because, among other things, it: (i) was too complex without assurances that it was sufficiently cost-effective; (ii) did not provide private sector companies sufficient flexibility to craft their own cybersecurity risk management assessment programs; and (iii) could create a perception that the Framework would lead to a path of compliance, benchmarking, or reporting by devising structured metric and measurement parameters that can be explicitly used to support external audits and conformity assessments. Assessments by other stakeholders were generally consistent with USTelecom's concerns.

Draft 2 does much to address these concerns, and USTelecom commends NIST for considering our and other stakeholders' constructive feedback. Draft 2's refined approach to metrics is evident at the outset with the retitling of Section 4.0 (at page 21) from "Measuring and Demonstrating Cybersecurity" to "Self-Assessing Cybersecurity Risk with the Framework." This simple change has significant consequences for the future use and perception of the Framework, as it signals that primary responsibility for assessing and mitigating cybersecurity risk continues to rest with individual organizations rather than some outside arbiter.

This theme is reinforced by the revised content of Section 4.0, which (at page 21) expressly eschews "reliance on artificial indicators of current state and progress in improving cybersecurity risk management" and cautions organizations to remain cognizant about "the

limitations of measurements" in this context. This section now concludes (at page 22) with guidance that encapsulates the themes that have girded the Framework since its inception: "Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations."

Draft 2's use of the companion "Roadmap" to elaborate on cybersecurity measurement is sensible as a matter of both substance and practice. Regarding the substance, Section 4.9 of the Roadmap properly recognizes that cybersecurity measurement is an evolving concept. As it aptly states (at page 14), "the broader issue of measurement" is "an under-developed topic, one in which there is not even a standard taxonomy for terms such as 'measurement' and 'metrics.'" The Roadmap goes on to say, "The development of reliable ways to measure risk and effectiveness would be a major advancement and contribution to the cybersecurity community."

USTelecom agrees, and as explained in our comments last year, that process requires ongoing dialogue between industry and government. USTelecom specifically proposed that NIST "undertake a separate initiative to establish criteria and a mechanism to evaluate the Framework's effectiveness over an ongoing period of time;" we also endorsed the recommendation by CSRIC IV Working Group 4 that organizations take under consideration NIST Special Publication 800-55 ("NIST SP 800-55") Revision 1 as an example of a good metric. Accordingly, USTelecom welcomes the Roadmap's notice (at pages 14-15) that NIST is "initiating a cybersecurity measurement program" to include consultation with the business, research, and government sectors, which will rely on NIST SP 800-55 among other existing work. USTelecom looks forward to continuing to work with NIST and other stakeholders during that process.

From a practical standpoint, the Roadmap's stated purpose (at page 1) is to house discussions of NIST's next steps with respect to the Framework and to identify "key areas of development, alignment, and collaboration" – presumably with greater ability for subsequent modification than is the case with the Framework itself. The addition of "Measuring Cybersecurity" to the list of topics addressed in the Roadmap (at pages 2 and 3) reinforces the acknowledgement that this issue remains very much a work-in-progress while more readily facilitating further updates as collaboration on this subject continues. Taken together, these and other aspects of Draft 2 return Framework Version 1.1's approach to measurement to the Framework's original vision and, in USTelecom's view, are far more likely to accomplish the central goal of promoting voluntary use of the Framework.

Conclusion

USTelecom and its members remain committed to the continued development, evolution, and implementation of the Framework and thus support NIST's efforts to update and enhance the Framework to ensure its effectiveness in the fluid and ever-changing cybersecurity landscape. USTelecom thanks NIST for its efforts to balance the need to update the Framework with the need for stability in doing so, and we look forward to continued and productive collaboration

with NIST, the Department of Commerce, and other government stakeholders as we undertake next steps together in the collaborative effort that has characterized the Framework's development since its inception. Please contact the undersigned if you have any questions regarding this submission or USTelecom's positions more generally.

Sincerely,

Robert Mayer
Senior Vice President – Cybersecurity