Before the
DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Washington, DC 20230

In the Matter of	)	
	)	
Evaluating and Improving NIST Cybersecurity	)	
Resources: The Cybersecurity Framework and	)	Docket No. 220210-0045
Cybersecurity Supply Chain Risk Management	)	
	)	

COMMENTS OF
USTELECOM—THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] submits these comments in response to the National Institute of Standards and Technology ("NIST") request for information in the above-captioned proceeding.[2] USTelecom recognizes the continuous value of the NIST Cybersecurity Framework ("CSF") developed in 2014, and we are proud to have contributed to the CSF's development in conjunction with USTelecom members and U.S. government partners.

Because the CSF was designed to be forward-looking and adaptable, avoiding the pitfalls of prescriptive and quickly outdated approaches, the CSF has withstood the test of time and USTelecom remains a strong proponent of this approach for mitigating organizational cybersecurity risks today.

[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 services to both urban and rural markets.

[2] *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, Docket No. 220210-0045 (rel. Feb. 22, 2022) ("CSF RFI").

The current CSF is effective and therefore changes should be minimal. If changes to the CSF are seen as unavoidable, however, then NIST should address backward compatibility issues, especially as related to other U.S. government efforts. It is particularly important to ensure that the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") can map its cross-sector control system cybersecurity performance goals and sector-specific performance goals to the CSF, without the mapping becoming obsolete a short while later.

While the CSF is flexible and highly effective, it competes with other frameworks for strained cyber resources. Therefore, mapping between the CSF and other approaches is essential. NIST should map the CSF to international standards, such as those of the International Organization for Standardization and the International Electrotechnical Commission ("ISO/IEC"). NIST should also map the CSF to supply chain risk management guidance, as detailed in these comments.

Given the CSF's success, USTelecom believes the CSF should serve as a model for risk management beyond cybersecurity. But the CSF should not itself be expanded to address non-cyber risks because doing so could hinder its cyber-specific utility.

USTelecom's long of history of collaboration with U.S. government partners informs our comments in these proceedings. In addition to helping NIST develop the CSF, we led the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC") landmark effort to implement the CSF in the communications sector.[3]

[3] *See* NIST, Cybersecurity Framework (last visited Sep. 7, 2021), https://www.nist.gov/cyberframework.

USTelecom presently chairs the Communications Sector Coordinating Council ("CSCC"), which is among the principal organizations serving as the government's industry partners for developing cybersecurity policies that affect the internet ecosystem. USTelecom founded, and presently co-leads with the Consumer Technology Association, the Council to Secure the Digital Economy ("CSDE"), a group of fifteen large international ICT companies dedicated to preserving the security of our communications infrastructure and connected digital ecosystem.[4] CSDE is recognized by the U.S. government as a leading industry partnership in coordinating efforts to combat botnets, respond to cyber crises, and promote cybersecurity through development of best practices that influence the development of standards.

As our leadership in these efforts makes clear, USTelecom fully recognizes the significant cybersecurity challenges facing our nation's infrastructure and broader stakeholder community, and we value the CSF for the role it plays in mitigating organizational cybersecurity risks. USTelecom is committed to finding proactive solutions that help NIST achieve its goals and offers these comments in the spirit of partnership and collaboration.

I. THE CURRENT NIST CYBERSECURITY FRAMEWORK IS EFFECTIVE AND THEREFORE CHANGES SHOULD BE MINIMAL

NIST asks whether any features of the CSF should be changed, added, or removed.[5] The CSF has served well in providing an effective framework for cybersecurity. The CSF has been embraced and utilized by a wide range of organizations both domestically and internationally. The CSF has formed the basis for many cybersecurity programs. As such, any changes to the CSF should, to every extent possible, be minimal, thoroughly considered and widely vetted.

[4] CSDE, https://csde.org.

[5] CSF RFI ¶ 4.

II. IF CHANGEES TO THE CYBERSECURITY FRAMEWORK ARE UNAVOIDABLE, NIST SHOULD ADDRESS BACKWARD COMPATIBILITY – ESPECIALLY AS IT RELATES TO OTHER U.S. GOVERNMENT EFFORTS.

NIST asks how changes to the CSF (functions, categories, subcategories, etc.) could impact the usability and backward compatibility of the CSF.[6] Should changes to the CSF be seen as unavoidable, those changes should indeed address backward compatibility and clear guidelines on impacts should be made available from the U.S. government.

In particular, NIST should coordinate with CISA, which is in the process of developing cross-sector control system cybersecurity performance goals as well as sector-specific performance goals, as called for by the July 28, 2021 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.[7] These goals should be mapped to the CSF to ensure that the broad community of security experts familiar with the CSF can reliably understand and implement the goals.

III. THE CYBERSECURITY FRAMEWORK SHOULD SERVE AS A MODEL FOR ADDRESSING RISKS BEYOND CYBERSECURITY, BUT SHOULD NOT BE EXPANDED TO ADDRESS NON-CYBER RISKS

NIST asks for suggestions to improve the alignment or integration of the CSF with other NIST risk management resources, such as the following:[8]

- NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286);

[6] *Id.* at ¶ 5.

[7] National Security Memorandum, *Improving Cybersecurity for Critical Infrastructure Control Systems* § 4(b) (July 28, 2021).

[8] CSF RFI ¶ 7.

- Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.
- Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

USTelecom believes the NIST CSF is appropriately focused on cyber risks. However, it is important to recognize the need for deeper engagement on other risks as well. Businesses face an array of financial, reputational, workforce, pandemic-related, and other risks. The CSF should not be expanded to address other risks, but rather should serve as a model for a voluntary, flexible framework. Moreover, concerns addressing risks outside of cybersecurity should be mapped by the U.S. government to the CSF.

USTelecom notes that mapping of the CSF to the Unified Compliance Framework: UCF Mapping Report for Improving Critical Infrastructure Cybersecurity, in particular, has been helpful to cybersecurity programs within our industry.

IV. THE CYBERSECURITY FRAMEWORK IS FLEXIBLE BUT COMPETES WITH OTHER FRAMEWORKS FOR STRAINED CYBER RESOURCES

NIST asks about the use of non-NIST frameworks or approaches in conjunction with the CSF, and specifically asks whether there are commonalities or conflicts between the CSF and other voluntary, consensus resources, as well as other government resources.[9]

[9] *Id.* at ¶ 8.

The significant list of non-NIST cybersecurity frameworks and approaches will compete for already strained cyber resources. Each framework and approach will require substantial knowledge and tracking of best practices toward compliance or accountability for all.

USTelecom notes again the importance of alignment between the CISA performance goals currently in development and the CSF, including cross-sector and sector-specific goals. Backward compatibility issues could arise if NIST were to make changes to the CSF functions, categories, subcategories that the CISA performance goals should map to.

The DoD Cybersecurity Maturity Model Certification (CMMC) serves as a good example of an effort where the U.S. government has supported industry implementation efforts by mapping compliance commitments between the CMMC 2.0 and CSF. As well, the CMMC 2.0 has been simplified – five levels have been reduced to three. The new levels are Level 1 (Foundational, basic cyber hygiene for handling of FCI per FAR 52.204-21), Level 2 (Advanced, NIST SP 800-171 for handling of CUI per DFARS 252.204-7012) and Level 3 (Expert, per NIST SP 800-172).

Such standardized mapping between CSF 2.0, and generally NIST SP 800-171, to non-NIST frameworks by the U.S. government is key to avoid an otherwise untenable task of each sector, and even each provider, having to model said linkages individually.

V. NIST SHOULD MAP THE CYBERSECURITY FRAMEWORK TO ISO/IEC STANDARDS.

USTelecom agrees with NIST that "continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services."

NIST asks what steps should be considered to increase international use of the CSF. As NIST notes, there are already numerous examples of international adaptations of the CSF by other countries. Similar to the mapping to U.S. government resources discussed above, mapping the CSF to ISO/IEC would be most effective in helping to increase international use of the CSF.

VI. NIST SHOULD MAP THE CYBERSECURITTY FRAMEWORK TO SUPPLY CHAIN RISK MANAGEMENT GUIDANCE

NIST asks whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework. USTelecom recommends that NIST update the Supply Chain Risk Management (ID.SC) informative references to include those references in particular that include the software supply chain work from the last four years. The updated references should reflect the following two documents with the third to be included once the final document is published.

1. NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, 2020 [SP 800-53]
2. NIST Special Publication 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (Feb 2022)
3. SP 800-161 Rev. 1 (Draft) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft)

VII. CONCLUSION

USTelecom appreciates this opportunity to comment on how NIST can update the CSF, which remains an incredibly valuable tool. We look forward to remaining engaged with NIST on this matter of significance to our members and the broader cyber ecosystem.

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler
Senior Director, Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

April 25, 2022