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

In the Matter of	)
	)
NIST Cybersecurity Framework 2.0	)
Concept Paper: Potential Significant	)
Updates to the Cybersecurity Framework	)
	)

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 feedback on the NIST Cybersecurity Framework 2.0 Concept Paper. USTelecom recognizes the continuous value of the NIST Cybersecurity Framework ("CSF"), 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Because the CSF was designed to be forward-looking and adaptable, avoiding the pitfalls of prescriptive and quickly outdated approaches, the CSF has withstood the test of time and USTelecom remains a strong proponent of this approach for mitigating organizational cybersecurity risks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.

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

[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.

Interoperability Council ("CSRIC") landmark effort to implement the CSF in the communications sector.[2]

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.[3] 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 offers these comments in the spirit of partnership and collaboration.

I. USTELECOM SUPPORTS APPLICATION OF THE CYBERSECURITY FRAMEWORK TO A BROADER SET OF CYBER RISKS

In the concept paper, NIST proposes that the CSF 2.0 will explicitly recognize the CSF's broad use beyond critical infrastructure. Among the measures proposed is to change the CSF's name officially to "Cybersecurity Framework" (which as NIST notes is already the commonly

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

used term). USTelecom supports this name change, as it acknowledges the reality of how the CSF has been widely applied by a broad variety of stakeholders.

II. USTELECOM SUPPORTS NIST'S PLAN TO INCREASE INTERNATIONAL COLLABORATION AND ENGAGEMENT—AND NIST SHOULD MAP THE CYBERSECURITY FRAMEWORK TO ISO/IEC STANDARDS

In the concept paper, NIST proposes a variety of measures to increase international collaboration and engagement. These measures are laudable, and in particular the work in the International Organization for Standardization (ISO) is important.

NIST should map the CSF 2.0 to ISO/IEC standards. This would be most effective in helping to further increase international use of the CSF. Not only are there numerous examples of international adaptations of the CSF by other countries, but also U.S. companies that operate internationally would benefit from such mapping.

III. THE CYBERSECURITY FRAMEWORK SHOULD CONTINUE TO ADDRESS GOVERNANCE WITHIN THE "IDENTIFY" FUNCTION—NOT CREATE A SEPARATE FUNCTION

USTelecom agrees with NIST that governance is an important feature of cybersecurity risk management. However, we believe it should continue to be addressed within the "Identify" Function, where it resides in the CSF 1.1, rather than create backward compatibility issues for a broad array of domestic and international stakeholders. On balance, the perceived benefits of giving "Governance" its own separate function are unclear and do not seem to outweigh the practical considerations and costs, both for the private sector and the government.

The CSF has been embraced and utilized by a wide range of organizations both domestically and internationally. Moreover, the CSF has formed the basis for many

cybersecurity programs. As such, any changes to the CSF Functions should be thoroughly considered and widely vetted.

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

In the concept paper, NIST proposes to map the CSF clearly to other NIST frameworks, while noting that these frameworks will remain separate. Conceptually, USTelecom believes this is the right approach.

As noted in our initial comments to NIST on the CSF 2.0 update, the 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, 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.

V. THE CYBERSECURITY FRAMEWORK SHOULD EMPHASIZE SUPPLY CHAIN RISK MANAGEMENT

In the concept paper, NIST states the CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management. To that end, NIST should 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 several years. The updated references should reflect the following three documents:

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 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

VI. 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
Vice President, Cybersecurity

USTelecom – The Broadband Association
[redacted]

March 3, 2023