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

In the Matter of	)
	)
Cybersecurity Framework 2.0 Public Draft	)
	)

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") on the Cybersecurity Framework ("CSF") 2.0 public draft. USTelecom commends NIST for its transparent, scientifically rigorous, collaborative partnership-based approach to developing the CSF 2.0. We believe that this update, to the extent it reflects the latest public draft, will help reinforce the CSF as the primary lens through which our industry and many other stakeholders view cybersecurity risk management, and our suggestions in these comments are intended to urge that result.

Specifically, we support NIST's current approach to addressing cybersecurity supply chain risk management ("C-SCRM") in a single category, as reflected in the latest draft. If needed, NIST can make reasonable changes to subcategories. But NIST should not create an entirely new and separate function for C-SCRM.

[1] USTelecom is the nation's leading trade association representing service providers and suppliers for the telecom industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse member base ranges from large international publicly traded communications corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country and world.

More generally, NIST should resist any calls at this time to add more functions to the CSF 2.0, as there has not been sufficient input, vetting, and discussion from the stakeholder community to support any major last-minute changes.

I. USTELECOM'S PARTNERSHIP WITH NIST AND THE U.S. GOVERNMENT ON CYBERSECURITY AND SUPPLY CHAIN SECURITY

USTelecom's long of history of collaboration with NIST and other U.S. government partners informs our comments in these proceedings. In addition to working with NIST on every iteration of the CSF since its inception more than a decade ago, USTelecom led the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC") landmark effort to implement the CSF in the communications sector. 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. 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.

II. RECOMMENDATIONS

1. NIST should address cybersecurity supply chain issues in the manner NIST has proposed in the public draft, rather than creating a new separate function.

As co-chair of the DHS ICT Supply Chain Risk Management ("SCRM") Task Force, USTelecom recognizes the importance of ensuring the security and resiliency of our nation's cyber supply chains. That is why USTelecom has continuously supported NIST's decision to emphasize SCRM in the CSF 2.0 by updating the Supply Chain Risk Management (ID.SC) informative references to include those references in particular that incorporate the software supply chain work from the last several years. We thank NIST for following through on our recommendations and believe this will increase the utility of the CSF.[2]

On balance, however, the perceived benefits of giving supply chain security 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.

To begin with, it would have an impact on backward compatibility. Keeping the supply chain elements where they currently reside would help minimize backward compatibility issues for a broad array of domestic and international stakeholders. Indeed, the CSF has been embraced and utilized by a wide range of organizations around the world as part of their cybersecurity programs. This tremendous success argues in favor of only making changes when clearly beneficial.

[2] USTelecom recommended the following informative references:

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

Secondly, the CSF is appropriately focused on cyber risks. And while cybersecurity and supply chain security are deeply connected, there are also key differences. We are concerned that elevating supply chain to a function would create confusion about the proper scope and therefore utility of the CSF. Alongside supply chain considerations, 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.

2. NIST should ensure any future proposed changes to the CSF Functions are widely vetted by the cyber expert community prior to considering adoption.

NIST is famous for its transparent, collaborative process where industry, government, and civil society come together to discuss proposals openly and pressure-test ideas to ensure that the best ideas rise to the top. In the course of updating the CSF to version 2.0, USTelecom, our members, and many other stakeholders have participated in multiple workshops and devoted substantial time and resources to working with NIST, enabling NIST to leverage insights from across the cyber expert community.

Making a major change like adding a function, at the last minute, would seem to circumvent this process and lead to questions about whether there has been an opportunity to appropriately vet the pros and cons of the proposal. As such, we urge NIST, at this time, to resist any calls to add more functions to the CSF 2.0, as there has not been sufficient input, vetting, and discussion to support major last-minute changes.

CONCLUSION

USTelecom appreciates this opportunity to express our support for NIST's current approach to updating the CSF. We look forward to continuing our collaboration with NIST on cybersecurity matters 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]

November 3, 2023