Before the
National Institute of Standards and Technology
Gaithersburg, MD 20899

In the Matter of

NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association (NTCA)[1] hereby submits these comments in response to the NIST request for input on the structure and direction of the Cybersecurity Framework (CSF or Framework) as it considers a draft of CFS 2.0. NTCA welcomes the opportunity to provide feedback on its proposals and is encouraged that NIST intends to maintain key attributes of the Framework – including its flexible, simple, and easy-to-use nature.[2] NTCA's members, all of which are small businesses and critical infrastructure providers serving rural America, appreciate NIST's focus on ensuring that the Framework remains scalable and flexible for a wide range of organizations.[3]

The overarching challenge for small communications providers implementing the CSF is the framework's length and complexity. While the CSF is necessarily broad in scope, it can nonetheless be overwhelming for smaller providers with limited resources to navigate as they

[1] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[2] NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework, p. 5 (January 19, 2023). (NIST Update Proposals)

[3] Id.

attempt to improve their cyber posture in accordance with the Framework. While the CSF is designed to be adaptable to companies of all sizes, many small and mid-sized communications providers do not have the time or expertise to identify which components of the CSF they can implement based upon current technical and financial capability, and they have described the guidance as overwhelming and time consuming. While the NIST Quick Start Guide for the CSF offers a short and easy to use method for companies of all sizes to implement the CSF, many smaller providers are either unaware of the Guide itself or how to utilize the Guide's recommendations despite the efforts of organizations like NTCA to spotlight the availability of such tools. Likewise, NIST's website contains a section for online learning that attempts to offer modules focused on different aspects of the CSF. However, the website does not make those modules readily accessible, and the topics included in each module are unclear.

To help small broadband providers understand and implement the Framework, NTCA, with the assistance of a member advisory group, developed a Sector Specific Guide to the NIST CSF for Small Service Providers. This guidance was reevaluated and updated in 2021 to reflect the evolving cybersecurity needs of small network service providers and our members' experiences with the NIST Framework.[4] NTCA also provides administrative and financial support for CyberShare: The Small Broadband Provider ISAC. This Information and Analysis Center offers cybersecurity support and information sharing to its participants. NTCA encourages NIST to engage with organizations serving critical infrastructure, such as NTCA and CyberShare, to help educate cybersecurity professionals within their sector about the changes to the Framework and to provide resources to help organizations develop resources that are tailored

[4] *See*, https://www.ntca.org/sites/default/files/documents/2021-08/NTCA%20Cybersecurity%20Series%20Part%203.pdf

to the sector and that offer more specificity than what NIST is able to offer. In short, as applied to small businesses, there is likely less need to modify the Framework itself (or certainly to issue new mandates), and more attention should be paid instead to alerting small businesses to the importance of the CSF and making it more navigable and implementable for these small businesses. If the "awareness, understanding, and adoption" barriers cannot be surmounted in the first instance, changing the underlying terms or issuing mandates of some kind cannot reasonably be expected to spur greater or more effective use of the Framework.

Relatedly, while it is intended that the Framework will remain scalable and flexible and its adoption voluntary, operating in accordance with it will nonetheless not be voluntary for many communications providers. For example, in order to participate in the Broadband Equity, Access and Deployment (BEAD) Program, broadband providers must attest to having plans in place that reflect the latest NIST Framework and the NIST Supply Chain Risk Management Guidelines.[5] The provider must also ensure that, to the extent they rely on network facilities owned or operated by a third party, they must obtain attestations from its network provider with respect to both cybersecurity and supply chain risk management practices. It is therefore important that NIST not inadvertently create unnecessary compliance standards that go beyond the CSF – and this highlights again the essential nature of giving smaller providers the ability to process the Framework and tools to implement it on a basis properly tailored for their circumstances.

[5] *See*, National Telecommunications and Information *Administration, Notice of Funding Opportunity, Broadband Equity, Access, and Deployment Program*, NTIA-BEAD-2022, pp 70-71 (May 13, 2022) , *See also*, NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* and related SCRM guidance from NIST, including NIST 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

The CSF 2.0 Concept Paper references other NIST cybersecurity and privacy-related frameworks that NIST indicates will remain separate frameworks. However, they will be referenced as guidance in CSF 2.0 or in companion materials.[6] Specifically mentioned are the Risk Management Framework, the Privacy Framework, the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity and the Secure Software Development Framework.[7] NIST is also collaborating to develop technology-specific mappings[8] and the Concept Paper references several documents that may "inform changes to the CSF."[9] NIST also seeks feedback on developing a template for organizations to develop CSF Profiles.[10] To avoid creating unnecessary additional burdens and to retain the flexibility of the CSF to the greatest extent possible, particularly for those companies that will be attesting to CSF compliance in connection with funding awards, it is imperative that the language of the Framework 2.0 makes clear that the references to additional guidance, resources, and materials are for informational purposes only and are not themselves part of the Framework. The Framework's greatest value is that it can be used by companies of nearly all types and sizes to enhance their cyber posture and that companies can scale it to their needs. To avoid whittling away at the stated voluntary – and importantly, flexible – nature of the CSF, NIST should take extra care to ensure that it remains something that providers can tailor to their operations and relative risk profiles, and NIST should not undermine its simplicity by sending companies down rabbit holes to now

6 NIST Update Proposals, p. 6.

7 Id.

8 Id. at 7

9 Id, pp. 7-8.

10 Id. at 9

comprehend and apply not only the CSF but also to develop expertise in several other documents, guides, and frameworks that may not be applicable or suitable to the needs of a particular organization.

Respectfully submitted,

By: */s/ Jill Canfield*
Jill Canfield
General Counsel, VP of Policy
[redacted]