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

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

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Request for Information ("RFI")[2] released by the National Institute for Standards and Technology ("NIST") in the above-captioned proceeding. NIST issued the RFI to seek feedback on measures that can be taken to update or modify the NIST Cybersecurity Framework ("CSF") "to account for the changing landscape of cybersecurity risks, technologies, and resources."[3] NTCA welcomes the opportunity to provide feedback and encourages NIST to ensure the CSF retains the CSF's voluntary nature and adaptability while also accounting for the needs and capabilities of, and risks and challenges faced by, small and mid-sized communications providers.

[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] *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management,* Request for Information*,* Docket No. 220210-0045, 87 FR 9579 (pub. Feb. 22, 2022).

[3] *Id.*

1. Current Benefits of Using the CSF (Q2)

NTIA sought feedback on the current benefits of using the CSF, including whether use of the CSF results in improved communications within and between organizations and entities (e.g., supply chain partners, customers, or insurers) and whether the CSF allows for better assessment of risks, improves effective management of risks, and/or increases the number of potential ways to manage risks.[4]

The CSF offers an important tool for supply chain security for several reasons, including due to the CSF's cross-sector applicability. Cybersecurity cannot operate in a silo, either within one organization or one type of industry.[5] The CSF was created as a voluntary framework with the need for such adaptability in mind. The guidance contained in the CSF is intended to be used by all critical infrastructure providers and adapted to their specific needs.

To help sustain such flexibility and adaptability, any cybersecurity or supply chain performance goals identified through this RFI must account for companies of all sizes. While the largest companies have substantial resources and personnel dedicated to cybersecurity, few small and mid-sized communications providers have even one employee dedicated to cybersecurity and have limited financial resources. The cybersecurity needs of, and challenges faced by, companies also vary widely. Accordingly, to be effective, the CSF must remain flexible enough

[4] *Id.*

[5] *See* Performance.gov, Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure Against Cyber Attacks and Other Hazards, available at https://obamaadministration.archives.performance.gov/content/goal-41-strengthen-security-and-resilience-critical-infrastructure-against-cyber-attacks-and.html (last visited Apr. 18, 2022) ("The concept of critical infrastructure as discrete, physical assets has become outdated as everything becomes linked to cyberspace.").

to allow all providers, including small and mid-sized providers, the ability to implement specific measures identified by the CSF in accordance with each company's needs and resources.

The scalability of the CSF, rather than a one size fits all approach, has been an essential feature of the CSF. The CSF's scalability has proven useful in allowing companies to adapt the CSF to the needs and capabilities of their own organization. In addition to remaining scalable, NTCA recommends the CSF continue to be made available in a manner that can be easily accessible and implemented by individuals without an information technology ("IT") or cybersecurity background. This is critical because small and mid-sized providers often do not have trained cybersecurity or IT professionals to manage their companies' cyber practices or the financial ability to purchase an extensive array of hardware, software or cloud-based tools. NTCA also urges maintaining the voluntary nature of the CSF. Maintaining this voluntary nature best allows companies of all sizes and scope to not only adapt the CSF to their present needs but also to readily adapt to the rapid and ongoing changes in technology without confusion as to what strict "compliance" may mean in any given context.

2. Challenges that may prevent organizations from using the CSF or using it more easily or extensively. (Q4)

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, small providers report being overwhelmed and lacking the necessary resources as they attempt to improve their cyber posture in accordance with the CSF. 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 have the technical and financial capability to implement and have described the guidance as overwhelming and time consuming. While the NIST Quick Start Guide for the CSF[6] offers a short and easy to use method for companies of all sizes, especially small companies, to implement the CSF, many smaller providers are either unaware of the Guide or of 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 purportedly offers modules focused on different aspects of the CSF.[7] However, the website does not make those modules readily accessible and the topics included in each module are unclear.

3. Additional ways in which NIST could improve the CSF, or make it more useful. (Q6)

NTCA encourages NIST to develop resources specifically intended to assist small and mid-sized providers implement the CSF while also reaching out to these providers through organizations like NTCA to make them aware of, and demonstrate how to utilize, these resources. The CSF can appear intimidating at first glance to individuals who are not trained in cybersecurity and, as noted above, even the web-based tools created to assist in understanding the CSF are themselves not user-friendly in all cases. Accordingly, providing video tutorials that guide small companies through how to identify and implement CSF tools that fit their needs along with a printed video guide that demonstrates, for example, how to document information flows, how to create firewalls, and how to detect unexpected data – and working through organizations like NTCA to educate on the use of such materials – would be more effective at increasing adoption of the CSF than creating new or additional text.

[6] Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide, NIST Special Publication 1271 (Aug. 2021), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf (last visited Apr. 18, 2022).

[7] *See* https://www.nist.gov/cyberframework/online-learning (last visited Apr. 18, 2025).

NTCA further encourages NIST to offer and publicize tools designed to help small and mid-sized providers understand and implement CSF components relevant to their operations. As noted previously, the Quick Start Guide offers even small companies a comprehensible starting point for implementing the CSF; however, a number of small and mid-sized providers are unaware of the Quick Start Guide. These providers are also likely unaware of the CSF tutorials posted on NIST's website. While these tutorials are not intended solely for small and mid-sized companies, smaller companies might benefit the most from the guidance as they typically do not have a team of in-house staff trained to help implement cybersecurity best practices. Even as NTCA itself does outreach to members to advise of the availability of such resources[8] (and is sure that other organizations in other sectors do the same), a renewed collaborative effort is likely needed to reach further into small business audiences.

To better ensure small and mid-sized providers are aware of resources intended to help them implement and benefit from the guidance provided by the CSF, NTCA encourages NIST to work with other government and private organizations to raise awareness of, and offer assistance with implementation of, the CSF.[9] The Small Business Administration and the American Farm Bureau Federation, along with C-SCRIP, could be effective ways to reach small companies with resources intended to help small companies apply the CSF to their operations.

[8] NTCA also developed a guide to the CSF intended specifically for small broadband providers. *See* Sector-Specific Guide to the Cybersecurity Framework, available at Cybersecurity Series | NTCA - The Rural Broadband Association (last visited Apr. 25, 2022).

[9] The National Telecommunications and Information Association's Communications Supply Chain Resource Program ("C-SCRIP"), for instance, seeks to "improve small and rural communications providers' and equipment suppliers' access to information about risks to key elements in their supply chain." As part of this effort, C-SCRIP has posted the Quick Start Guide on its website and has offered briefings for small communications providers to help them implement supply chain security. *See* https://www.ntia.doc.gov/cscrip (last visited Apr. 18, 2022).

Based on the foregoing, NTCA recommends NIST carefully consider how to make the CSF understandable and capable of being implemented, from a technical and financial perspective, for all companies, especially small and medium-sized providers. NTCA further encourages NIST to continue to make clear that the CSF is created and best positioned as a voluntary, rather than mandatory, framework in order to allow companies of all types and sizes the flexibility and incentive to adapt the CSF to their capabilities and needs.

Respectfully submitted,

NTCA THE RURAL BROADBAND ASSOCIATION

By: */s/ Tamber Ray*________
Jill Canfield
Tamber Ray
Roxanna Barboza

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
(703) 351-2000