Before the
National Institute of Standards and Technology, U.S. Department of Commerce
Gaithersburg, Md. 20899

In the Matter of	)	
	)	
Notice; Request for Information, Views on the Framework for Improving Critical Infrastructure Cybersecurity	))	Docket No. 151103999-5999-01

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association[1] ("NTCA") hereby submits these comments in response to the National Institute of Standards and Technology ("NIST" or "the Institute") Request for Information with respect to Views on the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework"), developed in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[2]

NTCA appreciates NIST's commitment to improving the nation's cybersecurity. The initial Framework has proven to be a useful tool in better focusing discussion and analysis of the nation's preparedness and resilience. Under immense scrutiny and a compressed timeline, NIST incorporated feedback from many varied stakeholders to create the Framework, which can guide critical thinking and implementation efforts across 16 critical infrastructure sectors and other diverse industries. Moving beyond the end product, NIST should be applauded for its interaction

[1] NTCA represents nearly 900 rural rate-of-return regulated telecommunications providers. NTCA's members help put rural Americans on an equal footing with their urban neighbors by providing broadband and other telecom services in high-cost rural and remote areas of the country. All of NTCA's members are full service local exchange carriers and broadband providers, and many of its members provide wireless, cable, satellite, and long distance and other competitive services to their communities. Each member is a "rural telephone company" as defined in the Communications Act of 1934, as amended.

[2] *Request for Information ("RFI"), Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Docket No. 151103999-5999-01.

with industry participants through an extensive multi-stakeholder, collaborative process, which addressed diverse requirements from its users.[3]

In regard to updates or edits to the substance of the Framework, including the Functions, Categories, Subcategories, and Tiers, NTCA urges NIST to refrain from making any substantive changes at this point in time. The Framework carefully balances the need for specific risk management-based activities, while also providing flexibility for interpretation based upon an organization's unique mission and environment. As a byproduct, the Framework is future-proof, in that even as threats and attackers evolve, risk-management strategies stand the test of time, continuing to address the evolving operational security requirements of organizations.

The Framework is designed to drive operators toward continual improvement, and constant attempts at re-evaluating and then subsequently updating the Framework would distract from the actual improvements already encouraged in the document. In addition, it is not practical or realistic to overhaul the Framework every two years, as it would be virtually impossible to "minimize disruption for those currently using the Framework"[4] as well as those working to understand and apply it to their operations. NIST and its partners would be stuck in a perpetual, vicious evaluation cycle, followed by individual sectors updating and refining their sector-specific guidance documents to align with the newly updated Framework, itself a large and time-consuming task.

In lieu of edits to the Framework, NIST should focus instead on developing supporting materials and guidance that can further assist its industry partners, and, in particular, address the

[3] Given the success of the Framework development process, NIST is seeking to employ a similar public-private strategy in other cybersecurity research and development efforts: https://www.ntia.doc.gov/press-release/2015/iptf-seeks-comment-key-cybersecurity-issues

[4] *RFI, Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Question 15.

needs of small and mid-sized businesses ("SMBs") within the critical infrastructure sectors. As NTCA has previously noted, the Framework is expansive, and therefore overwhelming and difficult to digest for small businesses that lack operations and staff comparable in size and scope to larger firms.[5] The Communications Security, Reliability and Interoperability Council IV Working Group 4 ("CSRIC IV WG4"), an advisory council to the Federal Communications Commission, attempted to address this gap by developing Framework implementation guidance for communications operators, including a specific report section focused on the needs of SMBs within the communications sector. However, given the complexity of the subject matter and inherent resource constraints, many small communications service providers will require additional guidance and supporting materials.

For instance, as NTCA has highlighted in the past, NIST should endeavor to document real-world use cases, i.e., the myriad of ways in which a critical infrastructure operator can apply the Framework within its operations.[6] As noted by various speakers at NIST outreach events, some operators are using the five main categories (Identify, Protect, Detect, Respond, and Recover), while others have undertaken the Framework process as initially intended and described within the document, creating a Current and Target Profile based upon the detailed 98 subcategories. These seemingly diverse ways to use the Framework are equally relevant, and offer much-needed assistance to small businesses. Likewise, the risk management approach espoused in the Framework may be new to some small businesses, as also noted at NIST events.

[5] Comments of NTCA, In the Matter of Request for Information, Experience with the Framework for Improving Critical Infrastructure Cybersecurity*,* Docket No. 140721609-4609-01; Comments of NTCA, In the Matter of Small Business Information Security; the Fundamentals, DRAFT NIST IR 7621 Rev. 1.

[6] The desire for documented real-world applications, case studies, and use cases has been noted within many forums, including NIST's December 5, 2014, Framework status update, available at: http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf

Small business may benefit from additional explanation with respect to what a risk-management approach entails. Further, NIST should explain how the Framework could be used alongside existing cybersecurity programs, processes, and industry and government standards. For instance, NTCA understands the Informative References section of the Framework is illustrative, rather than a comprehensive listing of all existing standards; however, it would be helpful to offer additional examples of how communications standards are aligned with the Framework subcategories, and how a communications operator that is already certified in an existing standard could adapt its cybersecurity program to fit the requirements of the Framework.

In addition to developing supporting documentation, small communications service providers need additional, in-depth technical training programs that are tailored to their specific needs. NTCA appreciates the Federal government's existing efforts to educate the public and private sectors at large, and, in particular, small businesses,[7] but many telecommunications companies are in need of more sophisticated training, including via one-on-one instruction.

NIST should partner with the Department of Homeland Security ("DHS"), Department of Commerce, and/or the Small Business Administration ("SBA") to develop a comprehensive Small Business Cyber Program. The Program should endeavor to aid small businesses in their use of the Framework, by first determining what gaps might persist in cyber practices, and then what practices (aka "incentives") might be helpful to address those gaps. This approach would dovetail with President Obama's February 9, 2016, Executive Order and related Fact Sheet that created the Cybersecurity National Action Plan ("CNAP"). The CNAP contains a long-term strategy and near-term actions for addressing the nation's shared cybersecurity posture, including

[7] NTCA also has engaged in a comprehensive outreach and education campaign to alert its members to the Framework and the key attributes of a risk-management cybersecurity program.

a SBA/NIST training program designed to reach small businesses through regional and district offices. NTCA looks forward to working with NIST to refine this program, and potentially adapt it for the specific needs of communications service providers.

As noted above, the concept of a Small Business Cyber Program evokes the need to revisit Framework "incentives" and how they can further encourage widespread use of the Framework by private industry. Indeed, although the Framework itself has been developed over time through an extensive process, the creation of adequate incentives has not come to fruition. Executive Order 13636 directed the Secretary of DHS to coordinate "the establishment of a set of incentives designed to promote participation in the [Cybersecurity] Program under development by NIST."[8] In a public document released in August 2013, the White House further acknowledged that barriers to use of the Framework exist and offered an initial examination of potential incentives, including insurance, liability protection, technical assistance,[9] rate regulation, and streamlining regulation,[10] which may serve to encourage small entities to further incorporate the Framework into their everyday business processes.

NTCA's members appreciate this forethought; however the term "incentives" is a mischaracterization. Managing cybersecurity risk is critical to the success of a small broadband service provider's business. To be successful and retain the confidence of its subscriber base, it is essential that all operators, large and small, maintain a secure network capable of transmitting

[8] Executive Order 13636, Sec. 8(d).

[9] Any government-led training or assistance aimed at facilitating use of the Framework should not be made contingent upon the collection of sensitive business data or any company-level identifiable information. Any such requirements could discourage small business participation and impede application efforts.

[10] Incentives to Support Adoption of the Cybersecurity Framework, The White House Blog, Released August 6, 2013, 11:04 a.m. EST (available at http://m.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework).

and receiving sensitive and personal data and information. However, some small operators face obstacles given their limited size and resources. Cost remains the single biggest barrier to use of the Framework by small communications carriers,[11] but the CSRIC Report outlines additional challenges inherent to a small communications operator, including limited access to operational manpower, the need for management buy-in, and the lack of available tools and resources needed to effectively and efficiently create, maintain, and evolve a cybersecurity risk management program, among other barriers.[12]

NIST should endeavor to reinvigorate the "incentive" discussion, joining forces with other Federal agencies and relevant associations to design and implement a set of incentives to encourage Framework use and overcome related barriers, especially those that are unique or disproportionately difficult for small entities. The Federal government should clearly define the breadth of incentives, the timeline of their availability, and how a small business can qualify for the incentives.

Finally, in regard to the long-term governance of the Framework, NTCA urges NIST to retain ownership and control of the Framework development process. Historically, small communications carriers have not had the financial, technical, and/or operational resources, to participate in standards-setting activities, which are managed by private-sector entities. This has led to the development of commercial standards that often do not account for the specific, discrete needs of small communications service providers. However, as noted above, NIST has established a collaborative relationship with its industry partners; helping to ensure that small

[11] *See* CSRIC IV, Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, March 2015, Sec. IX, 9.9, at page 204 and 206, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[12] *See* the CSRIC Report at 206 and 391.

companies needs and concerns will be heard and actively addressed by the Institute as it seeks to develop foundational cybersecurity best practices. To ensure the needs of SMBs continue to be met today and into the future, NIST should retain oversight of the Framework development process. However, if NIST decides to proceed with transitioning its governance responsibilities to another organization, at a minimum, the Institute should proceed with extreme caution, and an eye toward diversity and inclusivity as it seeks out a private-sector partner.

NTCA appreciates the opportunity to provide feedback. Cybersecurity is a shared responsibility, and the association looks forward to continuing its partnership with NIST to serve the cybersecurity needs of the consumers and businesses served by small communications operators.

Respectfully submitted,

NTCA THE RURAL BROADBAND ASSOCIATION

By: /s/Jill Canfield
Jill Canfield
Director, Legal & Industry
jcanfield@ntca.org

/s/Jesse Ward
Jesse Ward
Manager, Industry & Policy Analysis
jward@ntca.org

4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203
703-351-2000

February 23, 2016