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

In the Matter of:	)
	)
Request for Comments; Draft 2 of	)
Version 1.1 of the Proposed Update to	)
the Framework for Improving Critical	)
Infrastructure Cybersecurity	)

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION AND SUMMARY

NTCA–The Rural Broadband Association[1] ("NTCA") hereby submits these comments in response to the National Institute of Standards and Technology ("NIST" or "the Agency") request for public review and comments with respect to a Draft 2 of Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework"),[2] developed in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[3] and a draft version of a companion Roadmap for Framework evolution.[4]

[1] NTCA represents more than 850 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] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Draft 2, NIST, rel. Dec. 5, 2017: https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf. ("The Framework, Draft 2 of Version 1.1 with Mark-up").

[3] Executive Order 13636: "Improving Critical Infrastructure Cybersecurity," rel. Feb. 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. ("Executive Order 13636").

[4] Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, rel. Dec. 5, 2017: https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf. ("Roadmap").

As NTCA has emphasized in prior proceedings, the initial NIST Framework has proven useful in better focusing discussion and analysis of the nation's preparedness and resilience, providing a voluntary resource that can be used by a company of any size to help understand and reduce its cyber risk. NIST should be applauded for its interaction with industry participants, nurturing a true public-private partnership to successfully addresses diverse requirements. NTCA appreciates NIST's ongoing commitment to a multi-stakeholder approach, addressing the needs of varied organizations that have an interest in using the Framework internally within their operations to mitigate cyber risk.

The association appreciates NIST's revised second draft, which balances the needs of the user community by reducing interference with those currently using the tool while also proposing incremental edits to improve the document. Indeed, as NTCA highlighted in its February 2016 and April 2017 comments, any attempts to revise and update the resource should "minimize disruption for those currently using the Framework,"[5] as well as those working to understand and apply the Framework to their operations.[6] With any proposed update, the first valuable tenet is to "do no harm" to the existing resource and user base, and in that vein NIST has succeeded.[7] Likewise, NTCA appreciates that NIST has highlighted key topics in the Roadmap document for additional discussion, acknowledging several discrete issues which would benefit from further review and development including Measurement; Supply Chain Risk Management; and Small Business Awareness and Resources.

---

[5] *Request for Information ("RFI"), Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Docket No. 151103999-5999-01, rel. Dec. 11, 2015, Question 15.

[6] Comments of NTCA, *RFI, Views on the Framework for Improving Critical Infrastructure Cybersecurity*, at page 2; Comments of NTCA, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, 82 FR 8408, April 10, 2017, at page 3 ("NTCA's April 10, 2017 Comments").

[7] The Framework, Draft 2 of Version 1.1 with Mark-up, Note to Reviewers: "Version 1.1 is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective."

Moving beyond NTCA's general concurrence with the approach of Draft 2, the current Framework document could benefit from additional, iterative changes to provide valuable clarity and flexibility for small businesses. Section 4.0 is a vast improvement from its earlier state, ensuring that measurement is focused on *self-assessment* of internal cybersecurity risk management activities; however, the current draft provides limited direction as to how a user can specifically undertake the process of internally assessing its cyber risk management activities. Draft Section 4.0, therefore, offers limited value to NTCA's members and other small businesses on this complex topic. Given that the stakeholder community intends to further examine the issue though a more extensive public-private partnership review, as noted in the Roadmap, NIST should re-consider the inclusion of Section 4.0 into the Framework now. Instead, NIST should await feedback from the stakeholder community as to how an organization can measure its internal cyber risk management activities, and then leverage that input to provide more well-rounded and useful guidance for small businesses.

Likewise, NTCA appreciates that the supply chain guidance has been streamlined in Draft 2. However, NIST's guidance with respect to the supply chain remains more aspirational than realistic. NIST should re-examine its proposed guidance in relation to mitigating supply chain cyber risk in light of the inherent resource constraints and limited market leverage of small businesses. To be more useful to small businesses, NIST should provide practical, incremental actions that a small business can undertake to improve its supply chain risk management posture.

NTCA also appreciates the inclusion of Small Business Awareness and Resources within the Roadmap plan as a focus area in need of additional development. This focus on small businesses is consistent with NTCA's prior recommendations and with needs of the community, and the association looks forward to collaborating with NIST on small business outreach,

education, and resource development. However, NTCA also urges NIST to expand its small business program to address additional barriers to robust small business use through the development of a comprehensive "incentives" program, in collaboration with other Federal government partners.

II. REVISED SECTION 4.0 IS A VAST IMPROVEMENT, BUT NIST SHOULD POSTPONE INCLUDING ANY GUIDANCE WITH RESPECT TO SELF-MEASUREMENT UNTIL FURTHER DISCUSSION HAS TAKEN PLACE

In April 2017, NTCA submitted extensive comments regarding Section 4.0 as drafted in Version 1, and the association appreciates the revisions that have been since made to the document. From a macro level, the section has been renamed "Self-Assessing Cybersecurity Risk with the Framework."[8] The revised section heading more accurately reflects the needs of the user community, highlighting that *internal* assessments can impart significant value to an organization's security program. As NTCA affirmed in its April 2017 filing, some companies may benefit from a voluntary system or method to measure the effectiveness of an internal cybersecurity risk management program, and guidance on this topic would be appreciated.[9]

In addition, given the complexity of the topic, NIST appropriately cautions organizations as they seek to develop self-measurement strategies: "Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use…Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they

[8] The Framework, Draft 2 of Version 1.1 with Mark-Up, line 803.

[9] NTCA's April 10, 2017 Comments, page 5.

will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used."[10]

NTCA also appreciates that NIST has deleted Section 4.2 of Version 1.1 from the proposed update, previously entitled "Types of Cybersecurity Measurement," and that the topic has been highlighted within the Roadmap as an area in need of additional discussion and development. As conveyed by the community in written comments and workshop feedback,[11] measurement is a complex and controversial topic. The concept of self-measurement requires a methodical approach, including robust dialogue to ensure stakeholder consensus on any proposed guidance before it is introduced within the Framework document. This is consistent with NTCA's prior recommendations and the path espoused by NIST in the Roadmap.

NTCA looks forward to collaborating with the agency, and with the larger Framework community, to examine how measurement(s) and/or metric(s) can assist an organization with evaluating the effectiveness of its internal cybersecurity program in a manner that is consistent and provides flexibility to organizations of myriad sizes, levels of sophistication, and resources constraints. As NIST highlights, measurement "is an underdeveloped topic, one in which there is not even a standard taxonomy for terms such as 'measurement' and 'metrics.'"[12] Despite this challenge, NTCA agrees that "[t]he development of reliable ways to measure risk and effectiveness would be a major advancement and contribution to the cybersecurity

[10] The Framework, Draft 2 of Version 1.1 with Mark-Up, lines 834-837.

[11] See *Cybersecurity Workshop 2017 Summary*, rel. July 21, 2017, https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf, Section 4.1 Communications Sector Use, and Section 4.13: Measurement. Also see *Initial Analysis of Responses to Request for Comment (RFC) on Cybersecurity Framework Version 1.1 Draft Update*, rel. May 15, 2017, https://www.nist.gov/sites/default/files/documents/2017/05/16/rfc2-response-initial-analysis-20170515.pdf.

[12] Roadmap, Section 4.9: Measuring Cybersecurity, page 14

community."[13] At its heart, any discussion of metrics by NIST and/or within the Framework structure should address one fundamental question: is my organization's cybersecurity risk management program effectively mitigating risk to a level that is acceptable to my organization in a cost-efficient manner? Put another way, any metrics that are discussed or included within the Framework should attempt to address the success of a company's risk-management program, which is largely informed by its self-selected risk tolerance and tier structure, as highlighted in Section 4.0.

Despite NTCA's endorsement of the current direction of the measurement topic, the existing draft of the Framework could benefit from additional, iterative changes. Unfortunately, as currently written, Section 4.0 section provides minimal direction as to how self-measurement can be accomplished and scaled to organizations of various sizes and resource levels – and, therefore, is of limited value to NTCA members and small businesses like them. Although measurement is highlighted as an important aspect of an organization's risk management program, the Framework does not offer any practical guidance for how an organization can go about the process of undertaking effective measurement activities.

Further, some of the current language within Section 4.0 is vague and may leave users with questions. For instance, the concept of "lagging" and "leading" measurements are introduced without any elaboration as to the meaning of such terms.[14] NIST also includes the following example within the draft document, which uses opaque and confusing wording: "Making choices about how different portions of the cybersecurity operation should operate setting Framework Implementation Tiers."[15] It appears NIST may have intended to state that an

[13] *Id.*

[14] The Framework, Draft 2 of Version 1.1 with Mark-Up, line 841.

[15] *Id.*, lines 823-824.

organization may use the Framework Implementation Tiers to self-assess its cybersecurity program and its evolution – but this is an assumption, and the meaning is not entirely clear.

Given such concerns, NIST should revisit the inclusion of Section 4.0 within the document now. As discussed above, NTCA anticipates that additional direction may be forthcoming via Roadmap activities. Indeed, Section 4.0 likely will receive new edits as the topic is further discussed by the stakeholder community. Rather than rush to include the topic in Version 1.1, it may be better suited to address in a more comprehensive manner in future proposed updates.

III. NIST SHOULD ENSURE ITS PROPOSED GUIDANCE RELATED TO SUPPLY CHAIN RISK MANAGEMENT IS SCALABLE FOR ENTITIES OF ALL SIZES AND RESOURCE LIMITATIONS

With Draft 2 of the Framework, NIST has streamlined its guidance with respect to supply chain risk management ("SCRM"), including revised language within Section 3.3: Communicating Cybersecurity Requirements with Stakeholders, and Section 3.4: Buying Decisions. NTCA agrees that an important part of any cybersecurity risk management plan is the ability to identify, assess, and mitigate cyber risks derived from an organization's relationships with its suppliers, buyers, and partners. However, NTCA reiterates the concerns it first voiced back in April of 2017: NIST's proposed guidance continues to infer substantial responsibility on a company for the security of its supply chain, but without any accompanying discussion or recognition of a company's size and related resource constraints and market conditions.

Smaller telecommunications providers often have very few, if any options for suppliers that meet their needs, and extremely limited leverage in the marketplace to force suppliers to make necessary changes. For instance, NTCA's members may be unable to enact, communicate,

evaluate, verify, and validate cybersecurity requirements for their vendors.[16] As such, small businesses often may be unable to significantly influence the security of their supply chain partners and instead must look to identify and then mitigate the resultant risks internally.

To exacerbate matters, within the Framework Implementation Tier descriptions, NIST has provided limited options to characterize SCRM activities. In regard to supply chain activities, Tier 2: Risk Informed is characterized as the following: "the organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses, but does not act consistently or formally upon those risks."[17] And within Tier 3: Repeatable, SCRM is defined as the following: "The organization in response to events is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring."[18] Yet, there is nothing between the two tiers which offers realistic mitigation options to a small business which understands its supply chain risks, but has limited resources to address those risks. For instance, many small businesses likely do not have the market traction to force suppliers to entertain written, baseline agreements, or the resources to standup a governance structure allocated to cyber supply chain risk.

Indeed, within the Roadmap, NIST appropriately characterizes supply chain risk management activities, acknowledging that many organizations may find them challenging: "Although many organizations may have robust internal risk management processes, supply chain criticality and dependency analysis, collaboration, information sharing, supplier

[16] *Id.*, lines 687-693.

[17] *Id.*, lines 460-462.

[18] *Id.*, lines 482-486.

management, and trust mechanisms remain a challenge."[19] NTCA appreciates NIST's intent to provide the community with additional resources and guidance via future Roadmap activities.[20] Although it is important to challenge users to evolve their security programs, it would be more useful to provide additional, incremental actions small businesses can take to improve their supply chain cyber risk.

Narrowly within Section 3.4, NIST acknowledges that an organization may have to engage in some degree of "trade-off analysis"[21] in relation to buying decisions, "in that it may not be possible to impose a set of cybersecurity requirements on the supplier."[22] Rather, as NIST acknowledges, "the objective is to make the best buying decision among multiple suppliers, given a carefully determines list of cybersecurity requirements on the supplier."[23]

NTCA urges NIST to export this explicit recognition of market limitations to other areas of its SCRM advice. NIST should review its proposed guidance related to supply chain to ensure that its recommendations are scalable. To be useful to small businesses across various sectors, NIST should consider other steps an organization can take to improve its SCRM, providing recommendations that small business can strive for and realistically obtain within the marketplace.

[19] Roadmap, Section 4.4: Cyber Supply Chain Risk Management, page 7.

[20] *Id.*, pages 7-9.

[21] The Framework, Draft 2 of Version 1.1 with Mark-Up, line 725.

[22] *Id.*, lines 722-723.

[23] *Id.*, lines 723-725.

IV. NIST SHOULD EXPAND ITS SMALL BUSNESS PROGRAM TO FULLY ADDRESS BARRIERS TO USE, AND REINVIGORATE THE INCENTIVE DISCUSSION

NTCA applauds NIST for its commitment to Small Business Awareness and Education, as espoused in the Roadmap. Indeed, small businesses are a vital component of our nation's economy. Likewise, a "continued focus on cybersecurity best practices and implementation relative to small businesses is important to our Nation's cumulative cyber posture."[24] However, as NTCA has noted in prior proceedings, 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. [25]

NTCA appreciates the agency's longstanding commitment to small business outreach, including NIST's active participation in several NTCA-led events, U.S. Chamber of Commerce regional workshops, and now its partnership with the National Cyber Security Alliance on a webinar series. Further, as evidenced by the Roadmap, NIST plans to "embark on a 'listening tour' to hear first-hand from SMB [small and medium-sized business] owners about their cybersecurity needs," and then develop subsequent resources to address those needs.[26] NTCA agrees that development of those future resources should "reflect the specific preferences of those SMBs in determining" what shape and format those resources should take.[27]

As part of its small business resource development efforts, NIST should consider documenting real-world use cases, i.e., the myriad of ways in which a critical infrastructure

[24] Roadmap, Section 3: Evolution of the Roadmap, page 3.

[25] 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; NTCA's April 10, 2017 Comments.

[26] Roadmap, 4.12. Small Business Awareness and Resources, page 17.

[27] *Id.*

operator can apply the Framework within its operations.[28] As noted by various speakers at NIST-led events, some operators are using the five main categories (Identify, Protect, Detect, Respond, and Recover), while others have undertaken the Framework process as initially 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. 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.

NTCA looks forward to collaborating with NIST to further strengthen awareness and understanding of the Framework, including via the development of various resources small businesses may need to improve their cyber posture.[29] Moving beyond outreach and resource

[28] 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 (http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf) and NIST's more recent July 21, 2017 workshop summary (https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf).

[29] 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. In 2016 alone, more than 2,000

development, NTCA urges the agency to expand its small business program to fully addresses the myriad of barriers to robust small business Framework use. For instance, some small operators may need assistance overcoming obstacles given their limited size and resources, in addition to the complexity of the subject matter. Financial cost remains the single biggest barrier to use of the Framework by small communications carriers.[30] In addition, small companies experience challenges when attempting to analyze financial benefit or return on investment as it relates to cybersecurity. The Communications Security, Reliability and Interoperability Council IV Working Group 4 ("CSRIC IV WG4") Report on Cybersecurity Risk Management and Best Practices further enumerates additional challenges inherent to a small communications operator, including access to operational manpower, management buy-in, and the tools and resources needed to effectively and efficiently create, maintain, and evolve a cybersecurity risk management program, among other barriers.[31]

NIST, and its Federal government partners, should revisit Framework "incentives" and how they can promote more 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 remained somewhat of an afterthought and thus has not yet

attendees participated in a dozen NTCA-led events around the country. And in 2017, NTCA's Cybersecurity Summit and related online and in-person cybersecurity educational events drew more than 1,500 attendees. In addition, NTCA recently entered into a partnership with the Department of Homeland Security (DHS) and National Institute for Hometown Security to provide operators of small, rural telecommunications networks with robust educational programming and insights into industry best practices to aid their development of more comprehensive cybersecurity risk-management programs. The association's new cybersecurity education program, named NTCA CyberWise, is supported by an award through the DHS National Infrastructure Protection Plan Security and Resilience Challenge and the Office of Infrastructure Protection, in partnership with NIHS. The challenge provides opportunities for the critical infrastructure community to help develop technology, tools, processes and methods that address immediate needs and strengthen the long-term security and resilience of critical infrastructure.

[30] *See* the CSRIC IV WG4 Report at 204 and 206, available at: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[31] *Id.*, at 206 and 391.

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."[32] Further, it is well recognized that barriers to use of the Framework exist and potential incentives, including insurance, liability protection, technical assistance, rate regulation, and streamlining regulation,[33] are almost certainly required to encourage small entities to further incorporate the Framework into their everyday business processes. This being said, even 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, the small operator must maintain a secure network capable of transmitting and receiving sensitive and personal data and information.

NIST should endeavor to reinvigorate the "incentive" discussion, joining forces with other Federal agencies and relevant industry associations to design and implement a set of "incentives" that are designed 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 – and it must recognize that for resource-constrained small businesses, "incentives" will almost certainly need to take a different form than for larger firms. NTCA looks forward to assisting NIST and its government partners as

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

[33] Incentives to Support Adoption of the Cybersecurity Framework, The White House Blog, rel. August 6, 2013, 11:04 a.m. EST, available at: https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

they further evaluate tailored incentives to address the unique needs of small communications operators.

V. CONCLUSION

Cybersecurity is a shared responsibility and NTCA looks forward to continuing its partnership with NIST to serve the cybersecurity needs of small communications operators. Draft 2 is a vast improvement from the original proposed update; however, the current document could benefit from additional, iterative changes to provide valuable clarity and flexibility for small businesses. NIST should re-consider the inclusion of Section 4.0 into the Framework now. Regarding SCRM, the agency should strive to provide additional guidance within the document that can be scalded to organizations of all sizes and resources. Finally, as part and parcel of the Roadmap activities, NIST should expand its small business cyber program to collaborate with other Federal government stakeholders on the development of a comprehensive "incentives" program tailored specifically to address barriers to robust small business use of the Framework.

Respectfully submitted,

By: /s/Jilll Canfield
Vice President, Legal & Industry and Assistant
General Counsel
jcanfield@ntca.org

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

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