From: **Jesse Ward**
Date: Mon, Apr 10, 2017 at 2:58 PM
Subject: Comments of NTCA, Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Good afternoon,
Thank you for the opportunity to provide feedback.
Attached please find comments from NTCA–The Rural Broadband Association in response to the NIST Request for Comments (RFC) on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.
Please do not hesitate to contact me with any questions. I look forward to seeing you in May for the workshop.
Thanks,
Jesse

Jesse Ward
Director, Industry & Policy Analysis
NTCA–The Rural Broadband Association
4121 Wilson Blvd, Suite 1000
Arlington, VA 22203

[Attachment Copied Below]

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

In the Matter of:)
)
Request for Comments; Proposed) 82 FR 8408
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 Comments[2] with respect to a Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework"), developed in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

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 understand and reduce its cyber risk to an acceptable level. In addition, NIST should be applauded for its interaction with industry participants through an extensive multi-stakeholder, collaborative process, which addressed diverse requirements from its users.

[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] *Request for Comments ("RFC"), Proposed Update Framework for Improving Critical Infrastructure Cybersecurity*, 82 FR 8408, rel. Jan. 15, 2017.

NTCA appreciates NIST's ongoing commitment to a public-private partnership approach,[3] addressing the needs of varied organizations that have an interest in using the Framework internally to mitigate cybersecurity risk.

Before it makes any substantive changes to the Framework, NIST should ensure there is clear industry consensus on any proposed edits or additions. In addition, NIST should closely scrutinize any draft edits to the Framework to ensure they meet the foundational tenets valued by the user community; any changes to the Framework should ensure that the resource remains voluntary, adaptable to meet the evolving threat landscape, and flexible and scalable to meet the business requirements, operational needs, and resource limitations of various organizations. While evolution to anticipate and address new threats is an essential component of the Framework, changes must not disrupt the efforts of small businesses in particular to utilize the Framework.

Regarding specific changes to the Framework, NIST should decline to finalize its proposed language relating to metrics, i.e. Section 4.0 Measuring and Demonstrating Cybersecurity. Alternatively, NIST should convene a public-private working group composed of cross-sector representatives to further discuss a common methodology a company can use to internally measure the effectiveness of its cybersecurity risk management program. NIST also 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 instead provide additional activities that a small business can take to assess and mitigate cyber risks as they relate to suppliers, vendors, and partners.

[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

NTCA further reiterates its recommendation that NIST should endeavor to develop supporting material and guidance that can further assist its industry partners, and in particular, address the needs of small critical infrastructure providers. In addition, NIST should partner with the Department of Homeland Security ("DHS"), Department of Commerce ("DOC") 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.

II. CHANGES TO THE FRAMEWORK SHOULD ONLY BE MADE IF THERE IS CLEAR CONSENSUS, AND ANY EDITS SHOULD ADHERE TO THE FOUNDATIONAL PRINCIPLES OF FLEXIBILITY, SCALABILITY AND ADAPTABILITY

As a foundational matter, NTCA urges NIST to review its proposed changes to the Framework with an eye toward restraint and incremental improvement. As NTCA highlighted in its February 2016 comments, any attempts to revise and update the resource should "minimize disruption for those currently using the Framework,"4 as well as those working to understand and apply the Framework to their operations.5 NTCA appreciates NIST's efforts to update the tool; however, the Framework was inherently designed to be 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. Further, the Framework drives operators to continual improvement, urging a company to routinely re-examine the nature of its current cyber risks and the company's related mitigation activities. As such, constant attempts at

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

[5] Comments of NTCA, *RFI, Views on the Framework for Improving Critical Infrastructure Cybersecurity*, at 2.

re-evaluating and then subsequently updating the Framework itself threaten to distract from the actual improvements already encouraged in the document, and disrupt and undermine the efforts of those looking to leverage the Framework. In short, NIST should preserve continuity within the tool and closely examine any proposed updates to ensure they are necessary at this point in time.

In addition, before making any substantive changes to the Framework, NIST should ensure there is clear consensus on any proposed edits or additions that will assist and not hinder use of the tool. Formalized edits to the Framework should only be made to support those that currently use and/or are interested in using the Framework with managing their internal cybersecurity risk.

Finally, from a holistic viewpoint, as it seeks to refine and update the Framework, NIST should closely scrutinize any proposed edits to the Framework to ensure they align with the foundational principles valued by the user community. The Framework is a voluntary document, designed to be adaptable to address rapidly evolving attack parameters, and flexible and scalable so that it can individually tailored to meet an organization’s unique business requirements, operational needs, and resource limitations. The Framework must continue to carefully balance the need for specific risk management-based activities, while also providing flexibility for interpretation based upon an organization’s unique mission and environment.

III. NIST SHOULD DECLINE TO ADOPT SECTION 4.0 AS DRAFTED, AND INSTEAD CONVENE A PUBLIC-PRIVATE WORKING GROUP TO FURTHER DISCUSS HOW A COMPANY CAN MEASURE THE EFFECTIVENESS OF ITS INTERNAL CYBERSECURITY RISK MANAGEMENT PROGRAM

Regarding specific, proposed changes to the Framework, NTCA appreciates NIST's inclusion of Section 4.0, Measuring and Demonstrating Cybersecurity.6 Some companies may benefit from a voluntary system or method to measure the effectiveness of an internal cybersecurity risk management program. However, unfortunately NIST's proposed conclusions are premature and overly complex. This should not come as a surprise given the concept of metrics has produced widely varied feedback dating back to the initial development of the Framework. Taken into its totality, in the worst-case scenario, NIST's proposed metrics may have unintended consequences, including undermining private-sector voluntary use of Framework.

For instance, Section 4.0 refers to "external audits…and conformity assessments."7 Although these concepts are introduced as part of a broader, voluntary system of measuring and demonstrating cybersecurity, the mere mention of audits and assessments invokes a compliance-based checklist methodology. Audits are generally backward looking and focused on ensuring compliance with a prescriptive approach to security; they are designed to capture a company's compliance with a checklist of controls, versus the effectiveness of a company's approach or method of mitigating cyber risk. It is well settled that retreating to this type of approach would undermine the value inherent in the NIST Framework and its risk-management approach to security.

[6] The Framework, Draft Version 1.1, Section 4.0, available at: https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf.

[7] *Id.*, Lines 745-747.

In addition, Section 4.1 attempts to correlate cybersecurity metrics to business results. NTCA appreciates the reference to business outcomes, as a company's security program should be informed by its desired objectives. Put another way, cybersecurity should factor into every business decision a company undertakes, including mergers and acquisitions; the evaluation and/or launch of new products and services; and the acquisition of new software or hardware, to name a few. However, Section 4.1 quickly wades into the many details that influence a given business decision or outcome, of which cybersecurity is only one input. As NIST acknowledges, it is nearly impossible to quantify the correlation of cybersecurity to granular business outcomes.[8] Rather than proceed down this path, NIST should simply encourage companies to incorporate cybersecurity as part and parcel of any strategic business decision or process.

Further, NIST suggests that a company should measure the implementation of various specific cybersecurity controls versus holistically assessing the quality of the company's overall cybersecurity risk management program. In Section 4.2, NIST states that "[t]he cybersecurity outcomes of the Framework Core are the basis for a comprehensive set of cybersecurity management metrics. The aggregate of these metrics equals a reduction (or not) of cybersecurity risk."[9] In short, NIST seems to be suggesting that implementing additional security controls results in improved security. However, not all companies use all of the Framework

[8] *Id.*, Lines 778-792. NIST states, "The effect of a cybersecurity outcome on a business objective often may be unclear." (Line 792.) NIST also states that "[t]he ability of an organization to determine cause-and-effect relationships between cybersecurity outcomes and business objectives also depends on the ability to adequately isolate those cybersecurity outcomes and business objectives." (Lines 805-807). As a point of reference, NIST introduces an example which highlights how business outcomes may be impacted by many factors, of which cybersecurity is only one input: "For instance, a retail bank wanting to increase the number of online banking customers may seek to do so by implementing stronger authentication. However, achieving an increase in on-line banking customers is also contingent upon developing the messages regarding trusted on-line transactions, targeting specific demographics of consumers, selecting communication channels that are most meaningful to those demographics, and marketing those communication channels over a duration necessary to achieve the objective. In short, achieving customer growth is contingent on messaging, marketing, advertising cybersecurity, and other factors." (Lines 778-785.)

[9] *Id.*, Lines 829-831.

subcategories, and this does not mean that the company's given cybersecurity program is not efficient or effective at reducing the organization's cyber risk to an acceptable level.

Despite this blunt critique, NTCA agrees that the development of an internal metrics methodology may be useful to some companies, i.e. an accepted, proven, and foundational method that a company can use to measure its internal use of the Framework and its resultant effectiveness. In addition, NTCA appreciates the introduction of cost effectiveness as it relates to cybersecurity measurement,10 as cost is an important component of the evaluation and subsequent implementation decision.

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.

NTCA, therefore, recommends that NIST, in collaboration with its private-sector partners, further examine and study the issue of metrics as it relates to the NIST Cybersecurity Framework prior to making any metric-related changes to the Framework itself. The topic requires additional, robust dialogue in a collaborative approach with industry. NIST should convene a cross-sector, public-private working group that is tasked with further investigating and evaluating metrics or measurements that may assist a company with evaluating its internal progress.

[10] Id., Line 786: "The relative cost effectiveness of various cybersecurity activities is an important consideration."

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

NIST has incorporated references to supply chain risk management ("SCRM") throughout the Framework, including within the Framework Implementation Tiers (Section 2.2), recommendations regarding Communicating Cybersecurity Requirements with Stakeholders (Section 3.3), and the creation of a new section entitled Buying Decisions (Section 3.4). NTCA appreciates this forethought; 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, NIST's proposed guidance generally infers 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 are generally unable to negotiate, verify, and validate cybersecurity requirements for their vendors.[11] Also, smaller companies generally don't have resources to create a "Risk Council" entirely focused on the supply chain.[12] As such, small businesses often are unable to appropriately influence the security of their supply chain partners and instead must look to simply identify and then mitigate the resultant risks internally.

[11] See the Framework, Draft Version 1.,1, Section 3.3 Communications Cybersecurity Requirements with Stakeholders, Lines 610-617.

[12] *Id.*, as suggested in a proposed edit to Section 2.2 Framework Implementation Tiers: Tier 3: Repeatable, Cyber Supply Chain Risk Management, Lines 409-412: "An organization-wide approach to managing cyber supply chain risks is enacted via enterprise risk management policies, processes and procedures. This likely includes a governance structure (e.g. Risk Council) that manages cyber supply chain risks in balance with other enterprise risks."

Narrowly within Section 3.4, NIST acknowledges that an organization may have to engage in some degree of "trade-off analysis"[13] in relation to buying decisions, "in that it may not be possible to impose a set of cybersecurity requirements on the supplier."[14] Rather, as NIST acknowledges, "the objective is to make the best buying decision, optimally between multiple suppliers, given a pre-decided list of cybersecurity requirements."[15] Often that means that a "product or service is typically purchased with known gaps in its Target Profile," but an organization can address this residual risk through other management actions.[16]

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 that are realistically obtainable within the marketplace.

V. NIST SHOULD DEVELOP SUPPORTING MATERIALS AND GUIDANCE THAT CAN FURTHER ASSIST ITS INDUSTRY PARTNERS, AND, IN PARTICULAR, ADDRESS THE NEEDS OF SMALL CRITICAL INFRASTRUCTURE PROVIDERS

NTCA reiterates its recommendation that NIST should focus its efforts on developing supporting materials and guidance that can further assist its industry partners, and, in particular, address the needs of small and mid-sized businesses within the critical infrastructure sectors. As NTCA has noted in previous proceedings, the Framework is expansive, and therefore

[13] Id., Line 645.

[14] *Id*., Lines 642-643.

[15] Id., Lines 643-644.

[16] *Id*., Lines 645-646 and 651.

overwhelming and difficult to digest for small businesses that lack operations and staff comparable in size and scope to larger firms.[17] To address this challenge, as NTCA has previously suggested, 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.[18] 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. 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.

[17] 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.

[18] 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

VI. NIST SHOULD PARTNER WITH DHS, DOC, AND THE SBA TO DEVELOP A COMPREHENSIVE SMALL BUSINESS CYBER PROGRAM

In addition to developing supporting documentation, small communications service providers need additional, in-depth technical training programs, which 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; in fact, 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. But many companies may require more sophisticated and uniquely tailored programmatic training, including via one-on-one instruction.

NIST should partner with industry and government partners, including DHS, DOC, and/or the 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 dovetails with the executive order that first 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 a SBA/NIST training program designed to reach small businesses through regional and district offices. NTCA looks forward to assisting NIST with refining this program, and potentially adapting it for the specific needs of communications service providers.

Further, as noted above, the concept of a Small Business Cyber Program evokes the need to revisit Framework "incentives" and how they can further enable 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 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."[19] 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,[20] 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. However, 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.[21] 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

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

[20] 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.

[21] *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.

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.[22]

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

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

VII. CONCLUSION

Cybersecurity is a shared responsibility, and NTCA looks forward to continuing its partnership with NIST to serve the cybersecurity needs of the consumers and businesses served by small communications operators. As it seeks to refine and update the Framework, NIST should ensure there is clear consensus on any proposed changes before they are finalized, and that the tool continues to meet the needs of its industry partners. As such, NIST should refrain from issuing any recommendations related to measurement or metrics, i.e. proposed Section 4.0, and instead convene a working group to more closely examine the issue of metrics. Regarding supply chain, NIST should review its proposed changes to ensure that they are scalable for companies of all sizes. Finally, NIST should endeavor to lead the creation of a focused small business cyber program and related "incentives" tailored specifically for small businesses related to Framework use.

Respectfully submitted,

By: /s/Michael Romano
Senior Vice President, Industry Affairs and Business Development

/s/Jesse Ward
Director, Industry & Policy Analysis

4121 Wilson Boulevard, 10th Floor

Arlington, VA 22203