Before the
National Institute of Standards and Technology
Gaithersburg, Md. 20899

In the Matter of	)	
	)	
Notice; Request for Comments on the Preliminary Cybersecurity Framework	)	Docket No. 130909789-3789-01
	)	

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") Request for Comments on the preliminary version of the Cybersecurity Framework ("preliminary Framework"), which was developed in response to NIST responsibilities directed in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[2]

NTCA applauds the Federal government's efforts to develop a resource to assist critical infrastructure owners and operators with managing cybersecurity risk as part of an entity's normal business process. It is important to stress that any Cybersecurity Framework must be voluntary, consistent with Executive Order 13636.[3] Neither the Framework nor any related incentive should have the effect of turning suggested, voluntary guidelines into new unfunded

[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 Comments on the Preliminary Cybersecurity Framework*, Docket No. 130909789-3789-01, 78 FR 64478 (2013).

[3] Executive Order No. 13636, 78 Fed. Reg. 11739 (2013) ("Executive Order").

mandates on the communications industry or other sectors. NIST should incorporate additional guidance into the introductory language of the Framework affirmatively stating that adoption of the document is voluntary for all critical infrastructure owners and operators.

Furthermore, the Executive Order also notes that the Cybersecurity Framework should provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to identifying, assessing and managing cybersecurity risk.[4] Given these requirements, the preliminary Framework should more clearly recognize the limited resources of small entities by providing clarity and emphasizing cost effectiveness. Consistent with the Executive Order, the Framework also should incorporate flexibility to address the unique circumstances and needs of rural broadband providers. NIST should expressly indicate that entities are not expected to adopt all of the practices and standards enumerated in the document. The agency also should clarify that all critical infrastructure owners and operators that voluntarily adopt the Framework are not required or expected to reach the highest level of maturity as specified by the Framework Implementation Tiers ("FITs"). Rather, broadband service providers, especially those that are small businesses, should be encouraged to achieve the level that is appropriate for them, given their individual business needs and circumstances. Finally, to overcome barriers to adoption associated with lack of scope and scale, NIST should collaborate with the Department of Homeland Security ("DHS") to release the final Framework in concert with a rich set of incentives designed to encourage adoption of the document.

[4] Executive Order, Sec. 7(b).

II. THE GOVERNMENT SHOULD REFRAIN FROM ESTABLISHING UNFUNDED MANDATES

The Executive Order clearly notes that adoption of the Cybersecurity Framework should be voluntary for all critical infrastructure owners and operators.[5] As such, the Federal government, in carrying out the creation of the Framework, should refrain from an overly prescriptive document that effectively establishes new unfunded mandates, especially on small businesses in the communications industry and other sectors.

In various forums and meetings, NTCA has heard statements from the Administration that the Framework is not intended to function as a regulation, nor to result in any new regulations placed upon critical infrastructure owners and operators. However, despite these reassurances, there is no barrier to the adoption or incorporation of the Framework into existing or prospective regulatory structures. In fact, the Executive Order explicitly contemplates the potential for additional regulation to be imposed as an outgrowth of the Framework.[6] As such, NIST should provide clarity by incorporating additional guidance into the introductory language of the Framework affirmatively stating that adoption of the document is voluntary for all critical infrastructure owners and operators.

NTCA's members are small service providers that have limited resources. Although they have an admirable track record of efficiently leveraging every resource available to them, rural broadband providers face unique challenges associated with deploying and operating communications networks in areas characterized by low population density, often in remote

[5] Executive Order, Sec. 8(a).

[6] *Id.*, Sec. 10.

locations, that result in dramatically higher per-customer costs.[7] Any new unfunded regulatory mandates could add another level of uncertainty to the marketplace and divert already strained resources from important projects, such as broadband deployment and adoption efforts or maintenance of service reliability. Measures that would have the practical effect of imposing penalties against companies that elect not to follow some (or all) of the proposed Cybersecurity Framework would effectively force participation from all communications service providers, including small entities that already have stretched their thin resources to address routine operating and capital expenses.

The NIST Cybersecurity Framework and accompanying incentives may provide valuable tools for all critical infrastructure owners and operators. However, additional mandates are unnecessary to encourage rural broadband service providers to meet the needs of their customers. To adhere to the requirements of the Executive Order and ensure that small broadband service providers are able to maintain their focus on real-time security rather than static compliance, the Framework should stress the voluntary nature of its recommendations.

III. THE PRELIMINARY FRAMEWORK SHOULD MORE CLEARLY RECOGNIZE THE LIMITED RESOURCES OF SMALL ENTITIES BY PROVIDING CLARITY AND EMPHASIZING COST EFFECTIVENESS

In its current form, the preliminary Framework is overwhelming for small communications service providers that lack economies of scope and scale. The Framework

[7] Rural telecommunications providers also are facing unprecedented reductions in support and cost-recovery mechanisms that have heretofore allowed them to provide affordable telecommunications services available to consumers in all areas of the nation, pursuant to Sec. 254 of the Communications Act of 1934, as amended (47 U.S.C. Sec. 254). The resulting uncertainty has seriously impeded their ability to obtain financing necessary for subsequent investment in network infrastructure, and may threaten the ability to maintain broadband networks that exist today.

provides no guidance as to how small and rural broadband providers can cost-effectively implement their cybersecurity activities, as called for by the Executive Order.[8] Many of NTCA's members, in addition to being small businesses,[9] operate in extremely high-cost areas of the country with limited financial resources and staff members, often with fewer than 20 employees who each wear multiple hats with varied job responsibilities.

Given challenges related to their size and service territories, and shrinking cost recovery mechanisms in the wake of recent communications industry regulatory reforms, it is important that rural broadband service providers are provided with guidance on which recommendations listed in the Framework may be most effective. The Framework should clearly illustrate how a small service provider can substantively achieve the Framework's goals while also scaling down the number and complexity of steps needed to protect the operator's network from a cyber incident. In short, a straightforward "roadmap" is needed to help small companies process and interpret the document and the important issues it raises, thereby reducing the likelihood that small businesses will throw up their hands and do nothing instead in the face of an indecipherable and overly complex set of matrices with subparts, subcategories, and subtiers.

However, the preliminary Framework is difficult to use in current form. The sheer breadth and depth of information contained within the Framework is enough to discourage a small provider from investing scarce staff resources into adopting its recommendations, or even considering whether their current practices may already adhere to the Framework's suggestions. In addition to the Framework's three parts, four Elements, five Functions, four Tiers, and six

[8] Executive Order, Sec. 7(b).

[9] A local exchange carrier is considered to be "small" if it has fewer than 1,500 employees (13 C.F.R. § 121.201, 2007 NAICS code 517110).

Basic Steps, the Framework Core includes nearly 90 subcategories and many more citations to informative references and standards. Expansiveness may convey benefits, yet the preliminary Framework has attained this at the expense of clarity. As a result, it lacks a means to achievability. Without clear and realistic direction, rural broadband operators will be uncertain where to begin, and will likely be dissuaded from attempting to implement a bloated, confusing Framework given their size, resources, and other limitations.

The preliminary Framework also provides no insight into how critical cost-benefit analyses can be evaluated. A small company must be able to evaluate direct or indirect benefits to determine if the adoption of specific solutions, the costs associated with technology, people, and process enhancements, and the accompanying reduction in risk is, in sum, a cost-effective undertaking. The Executive Order specified that cost effectiveness should be a fundamental component of the Framework,[10] and it is especially important if the goal is to encourage cybersecurity considerations as part of an entity's routine business risk assessment processes. Further, more than ever, rural broadband providers need to perform critical cost-benefit analysis for every dollar spent.[11] In order to encourage small broadband service providers with limited resources to voluntarily evaluate and implement a new Cybersecurity Framework and incorporate it into a routine risk management process, the Framework should more clearly address concerns related to cost-effective implementation of the suggested guidelines and processes.

[10] Executive Order, Sec. 7(b).

[11] As evidenced by NTCA's member survey released January 2013, 69 percent of NTCA's member company respondents are being forced to postpone or cancel fixed network upgrades as a result of the uncertainty surrounding the Federal Communications Commission's ongoing Universal Service and Intercarrier Compensation reform efforts.

IV. THE FRAMEWORK SHOULD INCORPORATE FLEXIBILITY TO ADDRESS THE UNIQUE CIRCUMSTANCES AND NEEDS OF SMALL AND RURAL BROADBAND PROVIDERS

Flexibility is a key component enumerated in the Executive Order to describe the Cybersecurity Framework and its ability to adapt to different sized companies and various critical infrastructure sectors.[12] As such, the Framework should strive to maximize flexibility for rural broadband providers, recognizing their lack of scope and scale, their unique customer bases, and their ongoing commitment to maintaining secure networks.

A. The Framework Should Clearly Explain that Entities Are Not Expected to Adopt All of the Practices/Standards Enumerated in the Document

Based largely in the communities they serve, America's rural broadband providers have always displayed a strong commitment to responding effectively to the interests and needs of consumers, while simultaneously planning for, and appropriately reacting to, both potential and actual emergencies and threats involving their infrastructure and services. Managing cybersecurity risk is critical to the success of a rural broadband service provider's business. Precise security measures and practices are based upon a provider's unique market conditions and the individual needs of the provider's customers. Small entities must be able to retain this flexibility in order to respond to changing marketplace demands and evolving technological capabilities, as well as cyber-based threats.

Illustratively, the Federal Communications Commission's Network Reliability and Interoperability Council and its successor, the Communications, Security, Reliability, and Interoperability Council ("CSRIC") recognized that every best practice may not "be appropriate

[12] Executive Order, Sec. 7(b).

for every company in every circumstance."[13] Consistent with this finding, the Federal government should avoid adopting a Cybersecurity Framework that imposes adoption of *every* cyber best practice enumerated in the document; rather, a small broadband service provider should be expected to implement only those best practices or standards that align with the business needs and risks encountered by the provider and its specific customers.

As noted at recent NIST-led public workshops, the preliminary Framework is vague in defining what constitutes "adoption" or "implementation" of the Framework. Within the preliminary Framework itself, NIST states that organizations should have at least basic capabilities implemented in each of these areas of the five high-level sections in the Core: Identify, Protect, Detect, Respond, and Recover.[14] "Basic capabilities" can be widely interpreted and this may be appropriate. However, should the final version of the Framework and/or DHS, through its Voluntary Programs Working Group, provide further guidance on what "adoption" entails, the definition should incorporate maximum flexibility to account for the unique circumstances and lack of scale and scope experienced by small and rural broadband providers.

B. The Framework Should Clarify That All Critical Infrastructure Owners and Operators That Voluntarily Adopt the Framework Are Not Required to Reach the Highest Level of Maturity As Specified by the FITs

The final Cybersecurity Framework also should clarify that different entities can be at different FITs depending on their risk assessments, tolerances, and business needs. The term "Tier" inherently implies that an entity will be expected to move up the chain in maturity levels

[13] *See* CSRIC Working Group 2A, *Cyber Security Best Practices, Final Report* at 3 (Mar. 2011) (available at http://www.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf).

[14] Preliminary Framework, lines 397-401.

as time progresses. In describing the FIT, the Framework states: "[t]he Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4), progressing from informal, reactive implementations to approaches that are agile and risk-informed."[15] The term "progressive" is misleading and concerning for small entities. A more advanced Tier may not be appropriate given the entity's size, resources, and security risks. The Framework should consider small broadband service providers' unique circumstances when clarifying how critical infrastructure operators and owners should use the FITs.

V. NIST SHOULD COLLABORATE WITH DHS TO RELEASE THE FINAL FRAMEWORK IN CONCERT WITH A RICH SET OF INCENTIVES DESIGNED TO ENCOURAGE ADOPTION OF THE FRAMEWORK

The Executive Order 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."[16] NTCA members appreciate this forethought, as incentives that reward adoption are especially important given rural broadband service providers' lack of scope and scale and the complexity of the subject matter. In a public document released in August, the White House further acknowledged that barriers to adoption of the Cybersecurity Framework exist and offered an initial examination of potential incentives, including insurance, liability protection, technical assistance,[17] rate regulation, and streamlining regulation,[18] which may serve

[15] Preliminary Framework, line 157.

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

[17] Furthermore, any government-led training or assistance aimed at facilitating implementation 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 implementation efforts.

to entice small entities to further incorporate the NIST Cybersecurity Framework into their everyday business processes.

Although the Framework itself has been developed over time through an extensive process, the creation of adequate incentives has not yet come to fruition. In fact, the Voluntary Programs Working Group has held only two meetings since its inception. Given that adoption or implementation of the Framework has yet to be clearly defined, as previously discussed, the incentives thus associated with adoption, and how an entity qualifies for said incentives, are likewise murky. Unfortunately, the lack of clarity surrounding the government's creation and offering of incentives will significantly impede small entities' voluntary adoption of the Framework.

NIST should collaborate with DHS to release the final Framework in concert with a rich set of incentives designed to encourage adoption and to overcome barriers to adoption, especially those that are unique or disproportionately difficult for small entities. DHS and NIST should clearly define the breadth of incentives, the timeline of their availability, and how a small and rural broadband service provider can qualify for the incentives.

VI. CONCLUSION

NTCA recognizes the importance of securing our nation's critical infrastructure and appreciates the development of a voluntary Cybersecurity Framework that will provide practical advice and suggested guidelines. While it is essential that the public and private sectors work together to secure America's critical infrastructure, the Federal government should refrain from

[18] 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).

effectively establishing any new unfunded regulatory mandates on small entities. As small businesses based in the communities they serve, rural broadband service providers have strong incentives to ensure the security of their network users. Further, mandated compliance with any new Cybersecurity Framework would divert already-strained resources from important projects, such as broadband adoption and deployment in rural areas.

The Framework can be enhanced by redoubled efforts to emphasize the voluntary nature of the Framework, as well as flexibility and cost effectiveness. These are important attributes that are outlined in the Executive Order and listed as requirements of the NIST Cybersecurity Framework development process. The Framework should be easily scaled down for smaller entities, with clear-cut and straightforward guidance for how small and rural broadband providers can most effectively implement their cybersecurity activities and incorporate them into standard risk assessments. It should also provide insight into how critical cost-benefit analyses can be evaluated.

The Framework should maximize flexibility for small entities that face disproportionately high costs and limited financial and staff resources. It should clarify that critical infrastructure owners and operators are not expected to adopt all of the practices and standards enumerated in the document. Rather, the Framework should clearly note that a small broadband provider which voluntarily adopts the Cybersecurity Framework should only be expected to implement those best practices that align with the business needs and individual risks encountered by the provider and its specific customers. The Framework should also clarify that all entities are not required to reach the highest level of maturity as specified by the FITs.

In addition, the Federal government should provide clarity concerning the type of incentives available, the timeline when they will be available, and how a small entity can qualify for these benefits. Finally, the incentives should be available at the same time as the final Cybersecurity Framework is released.

Respectfully submitted,

By: /s/Jill Canfield
Jill Canfield
Director, Legal & Industry
NTCA–The Rural Broadband Association

By: /s/Jesse Ward
Jesse Ward
Manager, Industry & Policy Analysis
NTCA–The Rural Broadband Association

By: /s/Stephen Pastorkovich
Stephen Pastorkovich
Associate Director of Technology and Business Development
NTCA–The Rural Broadband Association

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