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

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Notice; Request for Information | ) | Docket No. 140721609-4609-01 |
| Experience with 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") Request for Information with respect to Experience with the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework"), which was developed in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" ("Executive Order").[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 remain voluntary, consistent with the spirit and the letter of the Executive Order.[3] In addition, it

[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, Experience with the Framework for Improving Critical Infrastructure Cybersecurity* Docket No. 140721609-4609-01.

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

would be a strategic mistake to simplify the Framework into a specific, prescribed set of static best practices, which can be readily identified by potential attackers. Further, cybersecurity mandates are unnecessary to encourage rural broadband service providers to meet the needs of their customers. 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. To ensure that small service providers are able to maintain their focus on real-time security, and adhere to the requirements of the Executive Order, NIST should ensure that future iterations of Framework remain voluntary, and stress the need for this course of action in its continued interactions with regulatory agencies.

The Framework was only officially released on February 12, 2014, a mere eight months earlier at the time of this writing. Before proceeding forward with additional recommendations, NIST and other various Federal agencies should allow adequate time for the communications industry to develop, sanction, and publicize sector-specific guidance through the Communications Security, Reliability and Interoperability Council ("CSRIC"), and, subsequent to the publication of CSRIC guidance, provide targeted direction to small businesses in particular and allocate additional time for small carriers to learn about and place the new recommendations into practice. This will provide small carriers with much-needed practical guidance in regard to how to digest the Framework and prioritize implementation of the numerous subcategories—an important requirement of the Executive Order.

NTCA has undertaken multiple education efforts to alert its members to the evolving nature of cybersecurity threats, the need for every communications carrier to adopt a cybersecurity risk management program, and the availability of Federal resources such as the Framework and the Department of Homeland Security ("DHS") Cyber Resilience Review ("CRR"). However, despite the variety of available Federal resources to assist small businesses with managing their cybersecurity risk, the message can appear muddled due to the number and complexity of Federal programs and initiatives, which rely on various references and provide similar yet varying guidance, without explanation for how the programs can work together.

The Federal government should coordinate and align its separate programs with respect to critical infrastructure cybersecurity, utilizing the same common taxonomy and lexicon as defined in the Framework and the overall structure of a risk management program likewise outlined in the Framework. This will provide clarity in regard to how various Federal programs can work together to assist small communications carriers. In addition, NIST, DHS, and the Federal Communications Commission ("FCC") should design and implement an integrated outreach, awareness, and education campaign to reach small businesses with one unified message with respect to cybersecurity risk management and recommended guidance for small communications carriers.

Finally, although CSRIC is attempting to address barriers to use of the Framework, small carriers will continue to face challenges, which stem from their lack of financial and operational resources. NIST should collaborate with DHS to release a rich set of incentives, which address the needs of small businesses, including technical assistance and cost recovery.

## II. TO ADHERE TO THE SPIRIT AND LETTER OF THE EXECUTIVE ORDER, NIST SHOULD ENSURE THAT FUTURE ITERATIONS OF FRAMEWORK REMAIN VOLUNTARY, AND STRESS THE NEED FOR THIS COURSE OF ACTION IN ITS CONTINUED INTERACTIONS WITH REGULATORY AGENCIES

The Executive Order clearly notes that adoption of the Cybersecurity Framework should be voluntary for all critical infrastructure owners and operators.[4] As such, the Federal government, in carrying out the ongoing evolution of the Framework and applicable sector-specific guidance, should refrain from developing overly prescriptive guidance that effectively establish new unfunded mandates, especially on small businesses.

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. Despite these reassurances, there is no barrier to the adoption or incorporation of the Framework into existing or prospective regulatory structures. However, it would be a mistake to simplify the Framework into a specific, prescribed, static set of cybersecurity best practices. Attackers are becoming more and more sophisticated, and, once they are aware that a communication's carrier—or the telecommunications industry as a whole—has implemented specific controls, they will revise their strategies to incorporate new methods, knowing that a carrier's resources are already tied up implementing the regulatory requirements. A far preferable approach is to allow organizations to perform their own individual risk assessments, and, based upon their unique threats and resultant

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

needs, implement appropriate cybersecurity best practices as they see fit based upon a menu of options, educational guidance, and other resources made available by the Federal government.

Cybersecurity mandates, in addition to being incongruent with the spirit and letter of the Executive Order, are unnecessary to encourage rural broadband service providers to meet the needs of their customers. 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 its 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 FCC's Network Reliability and Interoperability Council, and its successor CSRIC, recognized that every best practice may not "be appropriate for every company in every circumstance."[5] 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.

[5] *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).

In addition, to the extent that they have already put into place sufficient security protections to meet their individual business and customers' needs, the government should refrain from then placing additional mandates that defer resources from other critical projects. 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 locations, that result in dramatically higher per-customer costs.[6] 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 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.

To ensure that small service providers are able to maintain their focus on real-time security, and adhere to the requirements of the Executive Order, NIST should ensure that future

[6] 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.

iterations of Framework remain voluntary, and stress the need for this course of action in its continued interactions with regulatory agencies such as the FCC.

## III. THE FEDERAL GOVERNMENT SHOULD ALLOW ADEQUATE TIME FOR THE COMMUNICATIONS INDUSTRY TO DEVELOP, SANCTION, AND PUBLICIZE SECTOR-SPECIFIC GUIDANCE, AND FOR SMALL CARRIERS TO LEARN ABOUT AND PLACE THE FRAMEWORK INTO PRACTICE

In its current form, the Framework is flexible and scalable, but it is also expansive and, therefore, overwhelming and hard to digest for small businesses that lack economies of scope and scale comparable to the largest operators. The Framework does not provide direction as to how small businesses can cost-effectively implement their cybersecurity activities or how to prioritize implementation of the numerous subcategories contained within the Framework, both requirements of the Executive Order.[7] As such, small carriers are in needs of practical guidance for how they 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.

Many of NTCA's members, in addition to being small businesses,[8] 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

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

[8] 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). Few NTCA member firms even come close to approaching this threshold.

Framework may be most effective. In short, a straightforward "roadmap" is needed to help small companies process and interpret the document and the important issues it raises.

In its initial comments filed in this proceeding, NTCA suggested that NIST should revise the preliminary Framework to more clearly address the needs of small businesses and stakeholders' shared concerns related to cost-effective and prioritized implementation of the suggested guidelines and processes. Subsequent to this filing, NIST elected to release the Framework without addressing these issues, thereby hindering small company usability.

Sector-specific guidance may be able to fill in this gap in the agency's recommendations. Through the CSRIC IV Working Group 4, the communications industry is developing recommendations for small and medium businesses with respect to prioritization of relevant Framework categories and subcategories—a requirement of the Executive Order. This should provide small carriers with guidance in regard to where to start with using the Framework, while, at the same time, retaining flexibility for an individual company to interpret the Framework and how it can be placed into practice to meet the company's unique needs.

At the time of this writing, the Framework is only eight months old, and it will require additional time for the CSRIC IV cross-sector industry-working group to develop sector-specific guidance, and, thereby, adapt the NIST Framework to the communications sector. Further, once the industry best practices have been established, it will require more time—and, as discussed below, commitment on behalf of various organizations and federal entities—to educate small carriers with respect to the industry's revised approach to cybersecurity risk management and the availability of programs and resources to aid in implementing the CSRIC guidance.

Before proceeding with additional iterations of the Framework—or, in the case of regulatory and sector-specific agencies, cybersecurity regulatory requirements—NIST and various Federal agencies should allow adequate time for the communications industry to develop, sanction, and publicize sector-specific guidance through the CSRIC IV Working Group 4, and, subsequent to the publication of CSRIC guidance, allocate additional time for small carriers to learn about and place the new recommendations into practice.

## IV. THE FEDERAL GOVERNMENT SHOULD COORDINATE AND ALIGN ITS SEPARATE PROGRAMS WITH RESPECT TO THE FRAMEWORK, AND DESIGN A SINGULAR OUTREACH, AWARENESS, AND EDUCATION PROGRAM TO REACH SMALL BUSINESSES WITH ONE UNIFIED MESSAGE

NTCA has undertaken educational efforts to alert its members to the evolving nature of cybersecurity threats, the need for every communications carrier to adopt a cybersecurity risk management program, and the availability of Federal resources such as the Framework and the CRR. The Association has sponsored a variety of educational activities, including member webinars, presentations at regional conferences, and a general session industry speaker at NTCA's 2013 Annual Meeting. Likewise, NTCA applauds the outreach from the DHS Critical Infrastructure Cyber Community C3 Voluntary Program via a regional road show to engage in outreach and education for small businesses. And, as noted below, the CRR program is a significant asset for small businesses, which, oftentimes, are in need of technical assistance.

However, despite the variety of available Federal resources to assist small businesses with managing their cybersecurity risk, the message can be muddled due to the number and complexity of Federal programs and initiatives, which rely on various references and provide

similar yet varying guidance, without explanation for how the programs can work together. For instance, with respect to the Framework, the CRR, and the existing CSRIC III guidance, how do these programs vary in regard to their recommendations for small business? How do they overlap? What should a small business do first? If an entity is to take part in one program, or adopt one set of guidance, will it then be in compliance with the other resources?

As the Administration has noted in various forums, one of the strengths of the Framework is that it provides a common lexicon and taxonomy for various audiences within a company, and its vendors and consultants, to communicate in regard to cybersecurity risk. Likewise, with respect to cybersecurity, it is important that all Federal agencies and programs rely on this same common language and structure to ensure ease of communications and understanding. Further, although the communications industry is currently engaged in revising its sector-specific guidance via the CSRIC IV Working Group 4 undertaking, and its resultant guidance is designed to coincide with the Framework, it is critically important that this message is likewise conveyed to communications operators, i.e. CSRIC IV guidance is consistent with the Framework.

The Framework embodies a new risk management approach to cybersecurity. In regard to this new and improved paradigm, industry awareness and education is a process, a long-term undertaking that requires considerable time and patience. The foundation is a clear and concise message that is repetitively conveyed to industry in various forums and meetings. As such, the Federal government should coordinate and align its program with respect to the Framework, the CRR, and CSRIC guidance on best practices for cybersecurity; and, in addition, the Federal government—including NIST, DHS, the White House, and the FCC—should develop a joint

awareness, education, and outreach program based upon a common lexicon and taxonomy as outlined in the Framework.

## V. NIST SHOULD COLLABORATE WITH DHS TO SUPPORT USE OF THE FRAMEWORK BY SMALL BUSINESSES VIA A COMPREHENSIVE SET OF INCENTIVES DESIGNED TO OVERCOME COMMON BARRIERS TO ADOPTION FOR SMALL ENTITIES

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."[9] NTCA members appreciate this forethought, given rural broadband service providers' lack of scope and scale and the complexity of the subject matter. However, although the Federal government has often referred to the development of "incentives," this is the wrong characterization of the need for assistance. Rather, as previously noted, small communications carriers already strive to be as secure as possible with respect to their cyber operations, but given their lack of access to financial and operational assets, they are in need of support in regard to digesting and using the complex Framework.

CSRIC IV Working Group 4 is striving to minimize barriers to use of the Framework, including by simplifying the Framework into digestible bites; recommending how to use the resource within a company's operations; and suggesting prioritized implementation of the numerous subcategories within the Framework. However, small carriers will continue to face significant challenges in regard to organizational implementation of the CSRIC best practices, including the lack of financial resources to adopt various cybersecurity best practices and the

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

availability of affordable and accessible technical expertise. As such, the CRR, a program within DHS that provides free, confidential, on-site technical assistance to small businesses, is a valuable asset for NTCA's members. As noted above, NIST and DHS should align this program with the Framework, and subsequently publicize its availability and applicability to protecting core and critical infrastructure. In addition, NIST should collaborate with DHS to release a complimentary set of incentives designed to overcome additional barriers to adoption, especially those that are unique or disproportionately difficult for small entities.

In a public document released in August 2013, the White House acknowledged that barriers to adoption of the Cybersecurity Framework exist and offered an initial examination of potential incentives, including insurance, liability protection, technical assistance,[10] rate regulation, and streamlining regulation.[11] Although the Framework itself has been developed over time through an extensive process, the creation of adequate incentives has not yet come to fruition. 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. A diverse set of incentives is likely to appeal to a diverse set of companies with various operational challenges. Apart from technical assistance, small communications carriers are most in need of cost recovery for implementation of Framework activities.

[10] 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.

[11] 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).

## VI. CONCLUSION

NIST should adhere to the Executive Order and maintain the voluntary nature of the Framework in future versions of the document and in the agency's continued interactions with regulatory agencies. The Federal government also should allow adequate time for the communications industry to develop, publicize, and educate small businesses in regard to sector-specific, practical guidance with respect to how to use the Framework. In addition, the Federal government should coordinate and align its separate and existing initiatives with the Framework, the premier program for critical infrastructure operators and owners to manage cybersecurity risk. To reach small businesses with one unified message, the Federal government also should design a singular outreach, awareness, and education program. Finally, the Federal government should develop a rich set of incentives designed to overcome traditional barriers to implementation faced by small, resource-challenged organizations.

Respectfully submitted,

By: /s/Jill Canfield
Jill Canfield
Director, Legal & Industry
NTCA–The Rural Broadband Association
jcanfield@ntca.org

By: /s/Jesse Ward
Jesse Ward
Manager, Industry & Policy Analysis
NTCA–The Rural Broadband Association
jward@ntca.org

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