

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)
)
CSRIC IV Cybersecurity Risk) PS Docket No. 15-68
Management and Assurance)
Recommendations)

**REPLY COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION**

June 26, 2015

TABLE OF CONTENTS

	Page
I. INTRODUCTION & SUMMARY.....	1
II. THE CSRIC IV REPORT RECOMMENDATIONS ADDRESS THE STATED COMMISSION’S GOALS.....	3
III. THE COMMISSION SHOULD ALLOW ADEQUATE TIME FOR OUTREACH AND EDUCATION TO SMALL COMMUNICATIONS CARRIERS, AND FOR SMALL OPERATORS TO DIGEST AND PLACE THE NEW RECOMMENDATIONS INTO PRACTICE.....	6
IV. COMPANY-SPECIFIC MEETINGS SHOULD ONLY BE CONDUCTED ONCE SMALL CARRIERS ARE AWARE OF THE FRAMEWORK AND WG4 GUIDANCE AND UNDERSTAND HOW TO APPLY IT TO THEIR UNIQUE OPERATIONS.....	8
V. THE COMMISSION SHOULD COLLABORATE WITH DHS TO RELEASE A TAILORED SET OF INCENTIVES DESIGNED TO ENCOURAGE ADOPTION OF THE FRAMEWORK AND TO OVERCOME CHALLENGES NATIVE TO SMALL OPERATORS WITH LIMITED RESOURCES.....	10
VI. CONCLUSION.....	12

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)	
)	
CSRIC IV Cybersecurity Risk)	PS Docket No. 15-68
Management and Assurance)	
Recommendations)	

**REPLY COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION**

I. INTRODUCTION AND SUMMARY

NTCA–The Rural Broadband Association (“NTCA”),¹ hereby submits these reply comments in response to the Federal Communications Commission (“the Commission”) Public Notice² that seeks comment on the Cybersecurity Risk Management and Best Practices report (“Report”) submitted by the fourth Communications Security, Reliability and Interoperability Council (“CSRIC IV”).

The Report provides macro-level assurances that the communications industry is taking the necessary corporate and operational measures to manage cybersecurity risk across the enterprise. It also provides detailed, scalable guidance regarding how to apply the Framework

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 In the Matter of CSRIC IV Cybersecurity Risk Management and Assurance Recommendations, PS Docket No. 15-58 (March 19, 2015) (“Public Notice”).

for Improving Critical Infrastructure Cybersecurity Version 1.0 (“the Framework”)³ to protect an operator’s core network and critical infrastructure.

NTCA supports the Report’s recommendations and, consistent with the Executive Order that called for the Framework,⁴ urge the Commission to rely upon a voluntary, collaborative, flexible, operator-managed approach to cybersecurity matters as opposed to a traditional regulatory initiative. The record overwhelmingly supports that regulation is not needed to ensure communications operators commit to learning about and taking the necessary steps to adopt a risk-management approach to cybersecurity.⁵ Furthermore, as it looks to implement the Report’s recommendations, the Commission should ensure that the needs of and challenges faced by smaller communications carriers are taken into consideration.

NTCA’s members take proactive steps in regard to cybersecurity planning and operations.⁶ Indeed, managing cybersecurity risk is critical to the success of any service provider’s business. But the concepts introduced in the Framework and the Report are still nascent, and it will take smaller operators in particular more time to understand, digest, and apply these practices to their operations. As such, the Commission should allow adequate time for outreach and education by NTCA and other stakeholders, including the Commission itself and other Federal agencies with expertise in this area.

³ See “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.0, NIST, rel. February 12, 2014, available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

⁴ Executive Order 13636–Improving Critical Infrastructure Cybersecurity, Sec. 7(b), Rel. Feb. 19, 2013, <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

⁵ See the initial comments of CTIA – The Wireless Association; The Telecommunications Industry Association; American Cable Association (“ACA”); and the Satellite Industry Association.

⁶ For additional evidence of small operators’ commitment to cybersecurity planning and operations, see the initial comments of ACA and WTA – Advocates for Rural Broadband (“WTA”).

Further, the foundation of any successful education campaign is a clear and concise message that is consistently conveyed in various forums. To support this mission, the Commission should lend its support to the Department of Homeland Security's ("DHS") Critical Infrastructure Cyber Community C³ Voluntary Program ("C³ Program"). In addition, the Commission should collaborate with DHS to release a tailored set of incentives designed to overcome challenges inherent to small, resource-challenged organizations.

Company-specific meetings should only be conducted with small operators once they are aware of the Framework and the CSRIC IV Working Group 4 ("WG4") guidance, and have had the time to examine how it might apply it to their respective operations. In coordination with education efforts, the Commission should collaborate with industry associations to conduct an anonymous survey of small operators to ensure this first step has been achieved. Further, as a foundational matter, any and all company information gathered through any such process should be subject to the Protected Critical Infrastructure Information ("PCII") Program⁷ administered by the Department of Homeland Security ("DHS") or a legally sustainable equivalent.

II. THE CSRIC IV REPORT RECOMMENDATIONS ADDRESS THE COMMISSION'S STATED GOALS

Consistent with the multi-stakeholder collaborative approach used to create the Framework, NTCA applauds the Commission for convening WG4. More than 100 industry experts participated in the WG4 effort, representing all facets of the communications sector. Likewise, NTCA appreciates the Commission's ongoing support of a risk-management,

⁷ Department of Homeland Security, PCII Program, <http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program>.

outcomes-based approach to cybersecurity, consistent with the Framework that was the foundation for the WG4 effort.

WG4 was thereby charged with “ recommending voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across their respective enterprises.”⁸ To address this need, the Report suggested three new mechanisms, including: (1) FCC initiated confidential company-specific meetings; (2) a new component of the Communications Sector Annual Report that focuses on segment-specific cybersecurity risk management; and (3) active and dedicated participation in DHS’ C³Program. Taken together, the recommendations provide sufficient assurances that communications carriers of all sizes are adopting the Framework and the Report’s guidance.

In addition, WG4 was tasked with providing sector-specific guidance to assist communication providers with using the Framework. Of particular importance to NTCA and its small, rural members, WG4 convened a Small and Mid-Sized Business (“SMB”) Feeder Group to address the unique challenges and needs of SMBs within the sector.

The CSRIC Report provides essential guidance for small communications carriers. As NTCA has noted in other venues,⁹ in its current form, the Framework is flexible and scalable, but

⁸ Public Notice at 1.

⁹ See Comments of NTCA–The Rural Broadband Association, In the Matter of Small Business Information Security: The Fundamentals, DRAFT NIST IR 7621 Rev. 1, Before the National Institute of Standards and Technology, U.S. Department of Commerce, February 9, 2015. Also see Comments of NTCA–The Rural Broadband Association, In the Matter of Notice; Request for Information Experience with the Framework for Improving Critical Infrastructure Cybersecurity, Before the National Institute of Standards and Technology, U.S. Department of Commerce, October 14, 2014. And see Comments of NTCA–The Rural Broadband Association, In the Matter of Notice; Request for Comments on the Preliminary Cybersecurity Framework, Docket No. 130909789-3789-01, Before the National Institute of Standards and Technology, U.S. Department of Commerce, December 13, 2013.

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 apply their cybersecurity activities or how to prioritize use of the numerous subcategories contained within the Framework, both requirements of the Executive Order.¹⁰ Through the SMB Feeder Group, the CSRIC Report has now addressed this critical gap in application requirements.

The SMB section of the Report provides small carriers with direction in regard to where to start 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.¹¹ For instance, the SMB section includes a prioritized, culled list of Framework subcategories that is intended as a useful starting point for an SMB seeking to undertake a more formalized and structured risk management approach to protect its core network and critical infrastructure and services from cyber threats. The subcategory listing is merely illustrative and should not be boiled down to a comprehensive and inclusive list that pre-defines which NIST Framework subcategories necessarily apply to all SMBs within the communications sector. Rather, consistent with the NIST Framework, each company should examine its network, core business objectives/mission, risk tolerance, and security needs to determine which subcategories—of the 98 included in the NIST Framework—are most applicable to its operations.

¹⁰ See Executive Order 13636.

¹¹ See CSRIC IV, Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, March 2015, Sec. IX, 9.9, at page 370, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

Although the prioritized list may offer a helpful starting point for those SMBs intimately familiar with the NIST Framework, others will require more substantive guidance with simplified language and recommendations. As such, the SMB Feeder Group created narratives, using the subcategories as a guide, which are centered on three basic questions: (1) what does an SMB need to protect; (2) who has the responsibility for a given task; and (3) how will an SMB protect its core network and critical infrastructure and services (i.e. develop plans for identification, prevention, recovery, and continual improvement)? In addition, the SMB Feeder Group developed real-world use cases, which take multiple formats and are authored by operators of various sizes.

The entirety of the SMB Feeder Group’s analysis—including the illustrative subcategory listing; the “What,” “Who,” and “How” narratives; and the use cases—provide SMBs with direction in how they can apply the NIST Framework to protect their organizations’ core networks and critical infrastructure and services. And taken together, the Framework and the WG4 Report finally provide small carriers with much-needed practical guidance in regard to how to prioritize use of the numerous Framework subcategories—an important requirement of the Executive Order. But none of these elements was intended to serve as, and none is appropriate for service as, a comprehensive mandate for specific cybersecurity practices.

III. THE COMMISSION SHOULD ALLOW ADEQUATE TIME FOR OUTREACH AND EDUCATION TO SMALL COMMUNICATIONS CARRIERS, AND FOR SMALL OPERATORS TO DIGEST AND PLACE THE NEW RECOMMENDATIONS INTO PRACTICE

The Framework was only officially released on February 12, 2014, and the CSRIC IV WG4 segment-specific guidance with practical steps for small businesses was published online in March 2015, a mere three months before the time of this writing. As such, the underlying

risk-management approach to cybersecurity is still a nascent concept for all industry actors, and particularly for small, rural communications service providers. This new approach to cybersecurity will require significant commitment and collaboration on behalf of various organizations, including Federal entities, in order to appropriately educate small communications carriers. Before proceeding with company-specific one-on-one meetings, the Commission should allow adequate time for small, rural operators to learn about the Framework and the CSRIC Report, and then for each company to digest and place the new recommendations into practice.

NTCA remains dedicated to assisting its members in this arena. For example, NTCA has undertaken a comprehensive educational campaign 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, WG4 guidance, and C³ Program. Within the last two calendar years, cybersecurity risk management has appeared on the meeting agenda for every major NTCA-sponsored event, including presentations at NTCA's five Regional Meetings, NTCA's Annual Meeting, and the NTCA/NRTC 2015 IP Possibilities Conference & Expo, a flagship technical event attended by more than 400 participants, including technical staff members from small, rural broadband providers and the consulting community which caters to their needs. NTCA also convened a webinar, published a series of articles, developed an online resource center, and produced two videos introducing the benefits of the Framework and the CSRIC guidance to its membership. Additional activities are on the short-term horizon, as various aspects of cyber risk management

will be explored at an additional five industry events in late 2015 and early 2016, including the 2016 Wireless Symposium produced jointly by NTCA and the Rural Wireless Association.

There is clear interest in the topic and engagement from smaller providers, and NTCA is committed to educating its members with respect to the CSRIC recommendations. Likewise, in coordination with industry efforts, the Federal government—including the Commission and DHS—should develop a joint awareness, education, and outreach program based upon a common lexicon and taxonomy as outlined in the Framework.

Given that this is a wholesale change to cybersecurity practice and policy, industry awareness and education should be viewed as a process, a long-term undertaking that requires thoughtful planning, leadership from both industry groups and federal agencies, and, perhaps most importantly, considerable time and patience. Further, despite a strong commitment from NTCA and other the industry associations, some carriers may need additional incentives to overcome resource challenges native to small operations, as discussed below.

IV. COMPANY-SPECIFIC MEETINGS SHOULD ONLY BE CONDUCTED ONCE SMALL CARRIERS ARE AWARE OF THE FRAMEWORK AND WG4 GUIDANCE AND UNDERSTAND HOW TO APPLY IT TO THEIR UNIQUE OPERATIONS

Before undertaking further efforts to collect intelligence on the depth and breadth of industry use and adoption, including voluntary, invitation, company-specific meetings, the Commission needs to ensure that small operators are generally aware of Framework and the WG4 report, and also understand how to proceed forward using and applying the guidance within their unique operations. As such, in coordination with education efforts, the Commission should work with NTCA and other relevant associations to conduct an anonymous survey of small communications operators—not on the specifics of the Framework and CSRIC use within

their company, but rather on awareness of the risk-management approach and the segment-specific guidance as a threshold matter.

Moving forward, one-on-one voluntary meetings between the Commission, DHS, and small communications carriers should only be scheduled once awareness is raised, education is provided, and use of the CSRIC Report has sufficiently commenced within the small operator community. At that time, the Commission should review its experiences in regard to company-specific meetings with large operators and then apply those lessons learned to its engagement with smaller companies. The Associations also agree with the American Cable Association (“ACA”) in that the meeting topics should be broadened and organized as a two-way conversation, with an opportunity for the Federal government partners to impart information and best practices, and also learn from industry in regard to how government can assist their efforts.¹²

Further, as a foundational matter, any and all information gathered by the Commission in regard to cybersecurity planning and operations should be afforded protection under the PCII Program administered by DHS, or a legally sustainable equivalent. The PCII Program will provide operators with confidence that voluntarily participating in these meetings and sharing their information with the Federal government will not inadvertently expose sensitive or proprietary data, or leave them susceptible to future retaliatory action.

¹² See initial comments of ACA at 14-15.

V. THE COMMISSION SHOULD COLLABORATE WITH DHS TO RELEASE A TAILORED SET OF INCENTIVES DESIGNED TO ENCOURAGE ADOPTION OF THE FRAMEWORK AND TO OVERCOME CHALLENGES NATIVE TO SMALL OPERATORS WITH LIMITED RESOURCES.

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.”¹³ Further, in a public document released in August 2013, the White House further acknowledged that barriers to use of the Framework exist and offered an initial examination of potential incentives, including insurance, liability protection, technical assistance,¹⁴ rate regulation, and streamlining regulation,¹⁵ which may serve to encourage small entities to further incorporate the Framework into their everyday business processes.

NTCA’s members appreciate this forethought; however the term “incentives” is a mischaracterization. Managing cybersecurity risk is critical to the success of a small 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.

¹³ Executive Order, Sec. 8(d).

¹⁴ Furthermore, any government-led training or assistance aimed at facilitating use of the Framework should not be made contingent upon the collection of sensitive business data or any company-level identifiable information. Any such requirements could discourage small business participation and impede application efforts.

¹⁵ 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>).

NTCA agrees that financial cost remains the single biggest barrier to use of the Framework by small communications carriers.¹⁶ In addition, small companies experience challenges when attempting to analyze financial benefit or return on investment as it relates to cybersecurity. The CSRIC Report further enumerates additional challenges inherent to a small communications operator, including access to operational manpower, technical expertise, 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.¹⁷ As such, moving beyond basic outreach and education, many small companies may need one-on-one technical assistance to digest and apply the Framework and CSRIC guidance to their individual operations.

Although the Framework and segment-specific guidance has been developed over time through an extensive process, the creation of adequate incentives has not yet come to fruition. The Commission should collaborate with DHS, NTCA, and other industry associations to design and implement a set of incentives to encourage Framework use and overcome related barriers, especially those that are unique or disproportionately difficult for small entities. The Federal government should clearly define the breadth of incentives, the timeline of their availability, and how a small service provider can qualify for the incentives.

¹⁶ See the CSRIC Report at 204 and 206. *Also see* Comments of WTA at 10.

¹⁷ See the CSRIC Report at 206 and 391.

VI. CONCLUSION

For the aforementioned reasons, NTCA urges the Commission to continue to support a voluntary, flexible, and scalable approach to cybersecurity risk management. In terms of the CSRIC recommendations, small communications carriers are most in need of outreach and education. In addition, the Commission should collaborate to develop a tailored set of incentives to address small carrier resource limitations. As it looks to convene company-specific meetings, the FCC should, in conjunction with NTCA and other relevant industry associations, survey small companies to ensure that they are aware of the Framework and the CSRIC Report guidance. Voluntary, company-specific meetings with small carriers should only commence when a critical mass of small carriers has become aware of risk-management approach to cybersecurity and the resources available. Once this objective has been achieved, the Commission should look to the lessons it has learned with larger carriers. As a foundational matter, any information gathered by the Commission must be subject to PCII protection to ensure the safety and security of communications networks, and preserve the collaborative spirit of industry-regulator communications.

Respectfully submitted,

By: /s/Jill Canfield

Jill Canfield, Vice President, Legal and Industry &
Assistant General Counsel

Jesse Ward, Manager, Industry & Policy Analysis

NTCA–The Rural Broadband Association
4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203
703-351-2000