Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations	)	PS Docket No. 15-68

Comments of
WTA – Advocates for Rural Broadband

WTA – Advocates for Rural Broadband
Derrick B. Owens
Vice President of Government Affairs
Patricia Cave
Director of Government Affairs
317 Massachusetts Avenue N.E., Ste. 300C
Washington, DC 20002
(202) 548-0202

Dated: May 29, 2015

Table of Contents

Executive Summary……..…….…iii

I. Introduction……..…….…..2

II. More Time and Coordinated Outreach and Educational Efforts are Critical to Assist Small and Mid-Sized Telecommunications Providers in Bolstering Cybersecurity Risk Management and Best Practices…….……..…...5

III. Any Framework Established for Confidential Company-Specific Meetings and Sector Annual Report Must Ensure Inclusion of and Benefits for Small Broadband Providers…….….….8

IV. Remaining Financial and Practical Barriers Inhibit Effective Application of the NIST Cybersecurity Framework and Other Cybersecurity Risk Management Best Practices by Small Telecommunications Providers…....10

V. Conclusion …….……..…….…....13

EXECUTIVE SUMMARY

WTA supports an approach to the oversight and regulation of telecommunications provider cybersecurity risk management that avoids developing and imposing a prescriptive, cybersecurity check-list in favor of a more flexible, process-based risk management approach utilizing the NIST Cybersecurity Framework or other guidance resources as a starting point. WTA is pleased to note that the CSRIC IV's Report on Cybersecurity Risk Management and Best Practices includes a specific section for small and mid-sized telecommunications providers, highlighting that although small companies might lack resources, knowledge and training comparable to that of larger providers, they are a critical component of the overall framework for national and industry implementation of robust cybersecurity protections. Cybersecurity risk management outreach and education efforts are ongoing, and the Commission should allow sufficient time for providers to digest the Report's recommendations and assess their existing practices before taking additional steps toward regulating provider cybersecurity practices.

The recommendations on voluntary assurance measures contained in the Report are a great starting place for the discussion of how the communications sector can provide assurance of industry progress on cybersecurity risk management. However, further outreach to and inclusion of small providers is critical to ensure that consumers, businesses and service providers in rural areas benefit from broader industry efforts to improve cybersecurity practices, as well as protecting larger service providers that might have more sophisticated cybersecurity postures from cyber attacks initiated on small provider systems with which the larger providers interconnect.

Finally, as the Report notes, cost remains the single biggest barrier to implementing the NIST Framework and improving the adequacy of cybersecurity risk management technologies and practices in use by providers today. Other practical and legal barriers also influence industry adoption of cybersecurity risk management best practices. More progress on incentives is absolutely necessary to overcome financial and other barriers to improved cybersecurity.

Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations	)	PS Docket No. 15-68

Comments of
WTA – Advocates for Rural Broadband

WTA – Advocates for Rural Broadband ("WTA") hereby submits these comments in response to the Public Safety and Homeland Security Bureau's Public Notice[1] seeking comment on the report on Cybersecurity Risk Management and Best Practices submitted by the fourth Communications Security, Reliability and Interoperability Council ("CSRIC IV").[2] CSRIC IV was tasked with developing recommendations on how industry can provide demonstrable assurances that providers are reducing cybersecurity risks through the application of the voluntary National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework")[3] or an equivalent construct. The

[1] Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations, PS Docket No. 15-68, Public Notice, DA 15-354 (rel. Mar. 19, 2015) ("*Public Notice*").

[2] *See* CSRIC IV Working Group 4, Cybersecurity Risk Management and Best Practices Report (Mar. 19, 2015) *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf ("*CSRIC IV Report*").

[3] The National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014),

Bureau now seeks comment on the recommendations of CSRIC IV and/or suggestions of alternatives to better achieve the Commission's assurance goals.

I. Introduction

WTA is a national trade association representing more than 280 rural local exchange carriers ("RLECs") across the country. WTA's members are primarily very small entities with average staffs of between 7 to 15 employees. WTA's members serve expansive rural areas that have generally been financially unattractive to and disregarded by larger telecommunications carriers and cable operators due to their sparse populations, isolated locations, and/or rugged terrain that result in high costs and low profitability to provide service. Over the past decade or so, WTA members and other RLECs have increasingly been deploying fiber facilities and Internet Protocol ("IP") technologies further and further into their networks to meet the growing demand for broadband. WTA's members have vested interests in taking steps to ensure the availability and security of their networks because many RLECs provide services to critical facilities within their rural service territories including local government and public safety, power production and distribution, hospital and healthcare facilities, financial institutions, retail distribution centers, as well as schools and libraries.

WTA supports an approach to oversight and regulation of cybersecurity risk management that avoids developing and imposing a prescriptive, cybersecurity check-list in favor of a more flexible, process-based risk management approach utilizing the NIST Cybersecurity Framework or other guidance resources as a starting point. In addition to maintaining the flexibility to identify and address ever-changing threats, a non-

---

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021212.pdf ("NIST Cybersecurity Framework").

prescriptive approach will allow companies of all sizes to tailor their efforts toward utilizing available resources to address likely threats most relevant to their unique circumstances.

To the extent their resources permit, WTA members have tried to keep informed of likely threats and practices and the hardware and software available to defend against them. In most cases, the operators of critical facilities located in rural service areas assume primary responsibility for the firewalls, password protection systems and other cybersecurity defenses and practices used to protect their facilities. However, if and when problems arise, the local telecommunications provider is usually called in to assist with the defense, damage analysis and recovery efforts. Where feasible, some WTA members have installed session border controllers, intrusion detection systems, firewalls, flow analyzers, anti-virus software and other cybersecurity tools to offer protection for their networks and customers. Whereas WTA members can respond on an emergency basis to specific cyber attacks against their networks, they lack the resources – financial and personnel – to continuously monitor traffic flows in real time, to engage in measures such as deep packet inspection, or to devote substantial amounts of time to prospective planning, risk analysis and management, and cybersecurity training activities.

WTA is pleased to note that the CSRIC IV's Report on Cybersecurity Risk Management and Best Practices ("Report") includes a specific section for small and mid-sized telecommunications providers. This highlights recognition that small companies that might lack resources, knowledge and training comparable to those of larger providers are a critical component of the overall framework for national and industry implementation of robust cybersecurity protections. The Report adds much needed

simplification of the NIST Cybersecurity Framework for small providers into generic questions of "what," "who," and "how" such that the Report provides small companies a more workable analytical framework for assessing their current risk posture.[4] The Report also includes an important "Priority Practices" list that categorizes practices that the Small and Medium Business Feeder Group believed are the highest priority for companies to include in a risk management process.[5] Additionally, the Report contains a list of references and available resources companies can use to improve their cybersecurity practices.[6]

Consolidation of these kinds of resources into a single source is important for small telecommunications providers particularly as education and awareness remain major barriers to improved cybersecurity for small businesses and telecommunications providers. Industry outreach and education efforts are ongoing, and the Commission should allow sufficient time for providers to digest the Report's recommendations and assess their existing practices before taking additional steps toward regulating provider cybersecurity practices.

Likewise, the recommendations on voluntary assurance measures contained in the Report are a great starting place for the discussion of how the communications sector should proceed in assuring industry progress on cybersecurity risk management. However, the Commission must be mindful in implementing the recommendations to ensure that Department of Homeland Security ("DHS") and Commission education and outreach efforts on cybersecurity are effective in reaching targeted small and mid-sized

---

[4] *See CSRIC IV Report* at 377.

[5] *Id.* at 391.

[6] *Id.* at 393.

providers that most need the help. Further outreach to and inclusion of small providers is critical to ensure that consumers, businesses and service providers in rural areas benefit from broader industry efforts to improve cybersecurity practices, as well as protecting larger service providers that might have more sophisticated cybersecurity postures from cyber attacks initiated on small provider systems with which the larger providers interconnect.

Finally, as the Report notes, cost remains the single biggest barrier to implementing the NIST Framework and for improving the adequacy of cybersecurity risk management technologies and practices in use by providers today.[7] Other practical and legal barriers also influence industry adoption of cybersecurity risk management best practices. More progress on incentives is absolutely necessary to overcome financial and other barriers to improved cybersecurity.

II. More Coordinated Outreach and Educational Efforts are Critical to Assist Small and Mid-Sized Telecommunications Providers in Bolstering Cybersecurity Risk Management and Best Practices.

Beyond the cost of implementing any software and hardware solutions for improved cybersecurity and risk management, having appropriately trained employees is a cost that many telecommunications and non-telecommunications companies have yet to figure out how to manage. It is extremely rare for small telecommunications providers to have sufficient resources to hire dedicated cybersecurity or IT professionals or designate existing employees to focus solely on these issues on a full-time basis. As industry and policymakers alike recognize, the current demand for cybersecurity professionals with

[7] *Id.* at 27.

the requisite cybersecurity knowledge and skills far exceeds the available supply,[8] leaving small companies (and even the Federal, State and local governments at times) unable to be competitive in the marketplace for cybersecurity labor in light of the large salaries these professionals can demand from the national and multi-national corporations.

As a result, small companies rely heavily on freely available resources and outreach activities by industry groups, trade associations and the government to obtain the guidance they need to improve their cybersecurity risk management practices. While the Commission and DHS have tools for small businesses available online, substantially more proactive outreach and education is needed to ensure that companies are aware of not only what is expected of them with respect to cybersecurity best practices but also how they can meet those expectations without exceeding their limited budgets. Outreach to small businesses on cybersecurity risk management will be critical moving forward, especially as more companies seek to utilize the NIST Cybersecurity Framework and increase participation in cyber threat information sharing relationships.[9] Industry

---

[8] *See* Frost & Sullivan, *The 2015 (ISC)^2 Global Information Security Workforce Study*, 29 (2015), *available at* https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)²-Global-Information-Security-Workforce-Study-2015.pdf (finding that 62 percent of respondents in the telecommunications and media sectors lacked sufficient information security workers); RAND Corporation, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (2014), http://www.rand.org/pubs/research_reports/RR430 (analyzing the complexities behind the high demand and low supply of cybersecurity professionals); Adam Stone, *State and Local Governments Hustle to Fill the Cybersecurity Workforce Gap*, Government Technology (Oct. 3, 2014) *available at* http://www.govtech.com/security/Cybersecurity-Workforce-Gap.html (last accessed May 28, 2015).

[9] The CSRIC IV Report highlights the importance of cyber threat intelligence as a component of an effective risk management strategy for businesses and industry. However, small companies that lack experience and staff dedicated to cybersecurity and IT issues face difficulties in participating in information sharing in a meaningful way. Many less sophisticated companies are unsure of rudimentary aspects of cyber threat information sharing such as what information would be appropriate to share and what information should be acted on upon receipt. Guidance on best practices from government and the industry-at-large will be key to promoting small business involvement.

associations, like WTA, are moving forward with efforts to educate their members, in addition to outreach efforts by DHS and the Commission.

Although DHS has announced a small business outreach initiative through its C^3 Voluntary Program for 2015, no additional details have been released on what the initiative will entail and no outreach events been announced. Until such time that a more robust small business outreach plan and sufficient information is available for companies to know how they can meaningfully participate in the C^3 Voluntary Program, the Commission should refrain from using participation in C^3 activities as a way to evaluate assurances on cybersecurity, at least with respect to individual small telecommunications providers.

Furthermore, to the extent that the Report recommends "dedicated participation" it is important for the Commission to make clear what efforts suffice to meet that standard. For example, would use of the Cyber Resilience Review be sufficient?[10] Would companies be required to attend a certain number of educational events? Would attendance via webcast suffice? To the extent that RLECs are resource constrained both from a capital and human resource perspective, dictating how companies must participate in workshops and other events could unnecessarily divert resources away from improving security or inadvertently establish more of a compliance regime than is intended. The Commission should ensure that limited resources are used for making substantive improvements and progress on cybersecurity risk management practices and education.

[10] The Cyber Resilience Review is a no-cost, non-technical assessment tool that companies can use to assess their cybersecurity practices and operational resilience. Companies can do a self-assessment or have DHS cybersecurity professionals conduct an on-site assessment. https://www.us-cert.gov/ccubedvp/self-service-crr (last accessed May 28, 2015).

III. Any Framework Established for Confidential Company-Specific Meetings and Sector Annual Report Must Ensure Inclusion of and Benefits for Small Broadband Providers.

As its first recommendation for voluntary mechanisms to provide assurances that the communications sector is taking steps to enhance cybersecurity capabilities, CSRIC IV proposes that the Commission initiate company-specific, confidential meetings with providers to discuss their cybersecurity risk management practices and capabilities.[11] The Public Notice asks for input on "[h]ow . . . the Commission [should] prepare for and conduct these meetings to ensure that they result in information that is useful for assessing the state of cybersecurity risk management among communications providers[.]"[12]

As a starting point, the Commission should make clear its expectations regarding what is to be accomplished at the voluntary confidential meetings. What data should companies bring to illustrate their cybersecurity practices? In what format should companies present information to the Commission to ensure consideration of their cybersecurity efforts in the proper context of their unique circumstances? In order to make the meetings productive for the Commission as well as providers, expectations should be set and made known to the parties involved well in advance.

Additionally, companies will need to know what the Commission will do with information voluntarily provided in confidential meetings. Will the Commission retain records of the substance of the meetings? Will information provided to the Commission in meetings be used against the provider at a later date as evidence of adequate or inadequate security measures? How will the Commission develop requirements for

[11] *See CSRIC IV Report* at 7.

[12] *Public Notice* at 2.

confidential meetings without devolving the process into a check-list approach that would be inappropriate for assessing cybersecurity risk management? Without confidence that information shared in good faith will not be used for enforcement, companies may be far less likely (or altogether unwilling) to participate and detail their current practices at the risk of regulatory action for inadequate security standards.

Furthermore, the Report does not address any specific recommendations regarding the logistics of how, in practice, small providers can or should be included in such meetings. There are around 1,000 small telecommunications providers operating across the country, and it is unlikely that individual meetings with each company would provide benefits that would justify the expense to industry and the Commission. However, the Commission would do a disservice to these providers and their customers by failing to ensure that they have a seat at the table during discussions that likely precede steps in the regulatory process at a later date. With respect to these small service providers, the Commission must decide how it envisions company-specific meetings working. How will the Commission account for providers located in remote and rural areas and for whom traveling to Washington, DC for periodic meetings is impractical and costly but who might benefit the most from such meetings?

Developing the expectations and process for confidential meetings in such a way that includes and provides benefits for small telecommunications providers is critical especially if such meetings are to be used to assess the extent to which companies are ramping up their cybersecurity risk management efforts. Inclusion of small providers is particularly important if these meetings are preceded with the expectation that participation will stave off later imposition of a more prescriptive cybersecurity

regulatory regime for the communications sector. Meaningful inclusion of small providers in meetings to discuss progress on cybersecurity risk management is important to achieving the goals of obtaining assurances from industry and ultimately improving the cybersecurity posture of the sector as a whole.

Likewise, steps taken by small telecommunications to secure their networks should be included in any additional component to the Communications Sector Annual Report.[13] Just as the confidential, company-specific meetings could fail to adequately represent the interests and steps taken by the smallest providers, it is important that the Commission establish mechanisms by which small provider activities on cybersecurity are taken into account.

IV. Remaining Financial and Practical Barriers Inhibit Effective Application of the NIST Cybersecurity Framework and Other Cybersecurity Risk Management Best Practices by Small Telecommunications Providers.

Cost remains one of the biggest barriers to implementation of the NIST Framework and improved cybersecurity particularly for small telecommunications providers and small businesses more generally.[14] There are capital and operational expenses surrounding implementation of technologies, the NIST Framework and training staff.[15] Small companies in particular (and particularly those lacking employees with cybersecurity expertise) experience challenges when attempting to analyze financial benefit or any return from investments in cybersecurity.[16] Additionally, more resources

---

[13] *See CSRIC IV Report* at 7.

[14] *Id.* at 206.

[15] *Id.* at 212 (noting the CAPEX and OPEX costs associated with implementation and operation of SIEM/IPS/IDS technologies and systems for detection processes).

[16] *Id.* at 204 (noting that while large businesses see implementation of the NIST Framework as "a cost of doing business," the majority of small businesses see implementation as "a cost with no calculable direct return on investment").

are necessary for companies to be able to educate and train themselves and their employees on cybersecurity-related issues, including the application of the NIST Framework. As the Report notes, further work on developing market incentives for implementation of the NIST Framework and other cybersecurity risk management assessment tools and practices, including outreach and education efforts, is needed.[17] WTA agrees with the Report's recommendation that the Commission consider and advocate for the government at-large to develop economic incentives that would further NIST Framework adoption as well as adoption of improved cybersecurity risk management practices more generally.[18]

As the Commission is well aware, small telecommunications providers rely on subsidies from the Universal Service Fund ("USF") in order to make advanced telecommunications services a reality across the most rural and remote areas of the country. Since 2010, the Commission has been reforming the programs and support mechanisms within USF with an increasing emphasis on broadband Internet access and deployment of fiber optic networks. The Commission is still developing its reform plans for rate-of-return carriers. As cybersecurity and related issues become increasingly important for providers, it is similarly increasingly important that these costs at some point become part of the equation for the mechanisms providing support for telecommunications services in high-cost areas.

Purely financial constraints, however, are not the only barriers that remain. Small businesses and their employees (as well as consumers) are in need of education on cybersecurity and cyber-hygiene. Additional education is particularly important if the

---

[17] *Id.* at 214.

[18] *Id*.

Commission is to expect more proactive engagement by small providers on cyber threat information sharing. WTA's members are interested in the ability to share threat information and risk management practices with other carriers and the ability to evaluate their efforts against those of similarly situated companies and established industry standards. However, small providers that lack full time employees or assistance on cybersecurity and IT-related issues need guidance to understand and effectively participate in any cyber threat information sharing relationships.[19] Also, lack of education could subject a company to legal liability for mistakes made in the information sharing process. For example, employees lacking expertise might inadvertently share personal information of customers that is not necessary to identify a cyber threat. Likewise, an employee might lack the ability to recognize "actionable" threat information that has been shared with the provider until such information is no longer actionable.

The legal uncertainty involved with sharing information and the effect of insufficient cybersecurity knowledge currently outweighs the perceived benefits, particularly for small companies for whom consistent ex ante legal advice would be costly. There are efforts in Congress to provide a level of protection from liability for companies that share cyber threat information. The Commission should work together with industry to support these and other efforts to facilitate telecommunications industry participation in existing and new voluntary information sharing arrangements, including assisting small providers in understanding their role in the process.

[19] *See CSRIC IV Report* at 32 (recommending that the FCC encourage communications sector members to share relevant threat intelligence information with appropriate stakeholders in order to enable more efficient and scalable threat information gathering for use in threat analyses and cyber risk management decision-making).

V. Conclusion

WTA supports the Commission's current approach to regulating cybersecurity in the communications sector; more specifically WTA supports the decision to avoid utilization of a prescriptive, check-list style regulatory regime in this space. WTA commends the work of stakeholders in developing the CSRIC IV Cybersecurity Risk Management and Best Practices Report. The Report goes a long way towards making the NIST Cybersecurity Framework more relevant and workable for industry and for small telecommunications providers in particular. However, WTA recognizes that the work has just begun for improving cybersecurity risk management in the communications sector.

Existing and future outreach efforts by the Commission, DHS, and industry need to be better targeted to reach small providers, their employees and ultimately consumers. In light of the high cost and low return-on-investment for cybersecurity-related efforts and the inadequate supply of affordable cybersecurity professionals, resources and trainings made freely available by government and industry groups are vitally important for small companies to know what they can and should be doing to shore up the security of their networks within realistic budgetary constraints. This education and outreach is particularly critical in light of the financial barriers to implementation of the NIST Framework and cybersecurity-related technologies and practices, such as information sharing.

The Commission must also ensure that small telecommunications providers are included in the coordination of confidential, company-specific meetings with the Commission as recommended in the Report. Additionally, in order to make these

meetings productive for companies and the Commission alike, the Commission should make known its expectations for the meetings at the very beginning. Similarly, it is important that any addition to the Communications Sector Annual Report as recommended in the Report include cybersecurity network management contributions by small telecommunications providers and highlight steps they have taken to secure and improve their cybersecurity postures. Relying on company-specific meetings with the Commission and additional reporting by the communications sector in its Annual Report would not provide an accurate assessment of the state of industry commitment to cybersecurity if it failed to include representatives from the more than 1,000 small telecommunications providers providing service to millions of businesses and consumers across the country.

WTA and its members look forward to continuing to work with the Commission and other stakeholders in developing a targeted yet flexible regulatory approach and incentives that appropriately assists small telecommunications providers in meeting the cybersecurity challenges of the 21st Century.

Respectfully Submitted,

WTA – Advocates for Rural Broadband
By: /s/ Derrick B. Owens
Derrick B. Owens
Vice President of Government Affairs
317 Massachusetts Avenue N.E., Ste. 300C
Washington, DC 20002
(202) 548-0202

By: /s/ Patricia Cave
Patricia Cave
Director of Government Affairs
317 Massachusetts Avenue N.E., Ste. 300C
Washington, DC 20002
(202) 548-0202

Dated: May 29, 2015