Before the

National Institute of Standards and Technology, U.S. Department of Commerce

Gaithersburg, MD 20899

In the Matter of Notice: Views on the Framework for Improving Critical Infrastructure Cybersecurity	))))))))	Docket No. 151103999-5999-01

Comments of
WTA – Advocates for Rural Broadband

WTA – Advocates for Rural Broadband[1] ("WTA") hereby submits these comments in response to the National Institute of Technology ("NIST") Request for Information[2] with respect to industry views on the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework")[3] developed as a result of public and private sector collaboration pursuant to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" ("Executive Order").[4]

I. Any Future Versions of the Framework Must Remain Voluntary and Provide Sufficient Time for Small Businesses to Tailor Framework Adoption and Risk Management Best Practices Specific to Their Unique Circumstances.

[1] WTA – Advocates for Rural Broadband is a national trade association representing more than 300 rural telecommunications providers offering voice, broadband and video-related services in rural America. WTA members serve some of the most rural and hard-to-serve communities in the country and are providers of last resort to those communities. WTA's members are primarily very small telecommunications businesses with average staffs of between 7 to 15 employees.

[2] *Request for Information, Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Docket No. 151103999-5999-01, 80 Fed. Reg. 76934 (Dec. 11, 2015).

[3] The National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021212.pdf ("NIST Cybersecurity Framework").

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

WTA strongly believes that industry implementation of any current or future versions of the Framework *must* be voluntary. 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. 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, and to schools and libraries.

Whereas WTA members can and do respond on an emergency basis to specific cyber attacks against their networks, they for the most part lack the additional resources – financial and personnel – to devote substantial amounts of time to prospective planning, risk analysis and management, and cybersecurity training activities either in-house or through third-party vendors. Moreover the time that must be dedicated to comprehensive approaches to cybersecurity risk management places a substantial burden on small telecommunications carriers. While many WTA members have taken advantage of the Framework and sector-specific guidance to develop comprehensive risk management policies and procedures, others simply lack the resources and expertise to do so in the fashion as envisioned by the Framework.

A fundamental tenant of President Obama's Executive Order that initiated development of the Framework was that the Framework should be voluntary, flexible and scalable for critical

infrastructure owners and operators.[5] The voluntary nature of the Framework is fundamental, particularly in light of the very real resource constraints facing small telecommunications carriers. The paradigm within the Framework of a risk-based approach to mitigating cyber risks is a more effective approach toward improved security than application of prescriptive set of regulations and requirements to many uniquely situated entities. However, despite the purely voluntary nature of the Framework, the Federal Communications Commission ("Commission") tasked its fourth iteration of the Communications Security Reliability and Interoperability Council ("CSRIC IV") with developing recommendations on how the telecommunications industry can provide "demonstrable assurances" that providers are reducing cybersecurity risks, including through the application of the Framework.[6] NIST should continue to remind regulatory bodies at all levels of government that the Framework should be viewed solely as yet another tool available for assisting businesses in improving their cybersecurity risk management practices, rather than as a baseline for developing prescriptive security regulation or assessing a particular business' cybersecurity risk management practices.

NIST should also ensure that small businesses have sufficient time to digest the Framework and sector-specific guidance derived from the Framework before moving forward with comprehensive updates or re-writes of the Framework. WTA welcomed the release in March 2015 of the CSRIC Report on Cybersecurity Risk Management and Best Practices

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

[6] *See* 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*").

("CSRIC IV Report")[7] because it tailored application of the Framework for small and mid-sized telecommunications carriers. The CSRIC IV Report adds much needed simplification of the Framework for small providers into generic questions of "what," "who," and "how" such that it provides small carriers a more workable analytical framework for assessing their current risk posture than provided by the Framework alone.[8] The CSRIC IV Report also includes an important "Priority Practices" list that categorizes the Framework categories and subcategories that representatives of small and medium-sized businesses contributing to the CSRIC IV Report believe are the highest priority for companies to include in a risk management process.[9] Additionally, the CSRIC IV Report contains a list of references and available resources companies can use to improve their cybersecurity practices.[10] Consolidation of these kinds of resources into a single source is particularly helpful as education and awareness remain major barriers to improved cybersecurity for small businesses, including WTA's rural telecommunications provider members. However, the pure breadth of information available can be substantially overwhelming for businesses with fewer than 10 employees or those that lack employees dedicated solely to cyber-related issues.

Although industry outreach and education efforts are ongoing, shoring up cyber defenses and risk management practices has proven to be a struggle for public and private sector entities, large and small alike, and small businesses continue to need additional time to fully understand, evaluate and put into practice the Framework and other recommendations. Accordingly, NIST

---

[7] *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*").

[8] *Id* at 377.

[9] *Id.* at 391.

[10] *Id.* at 393.

should ensure that industry has had sufficient time to digest the Framework and other tools that aim to tailor the Framework's applicability to different industry sectors and business sizes before moving forward with substantial re-working or updates to the Framework.

Rather than pursuing updates to the Framework at this time, NIST should publicize a variety of illustrative use cases that would serve as examples for industry participants of all sectors and sizes in conducting risk assessments in accordance with the Framework along. The flexibility of use of the Framework has been a key attribute to success and publication of a range of examples would provide additional guidance for those entities that lack expertise to work with the Framework on their own.

II. Additional Work on Developing Incentives, Educating a Cybersecurity Workforce and Coordinating Outreach to Small Businesses is Critical to Support Effective Use of the Framework and Other Cybersecurity Risk Management Best Practices.

Cost remains one of the biggest barriers to implementation of the Framework and improved cybersecurity postures particularly for small telecommunications providers and small businesses more generally.[11] Small companies—particularly those lacking employees with cybersecurity expertise—experience challenges when attempting to analyze the financial benefit or any return from investments in cybersecurity, including review and application of the Framework.[12] Other companies might simply lack any additional resources necessary to take more than minimal steps toward securing their networks. For WTA's members, the availability of resources at this time for Framework implementation is unknown as a result of ongoing reforms to the Universal Service Fund's High Cost Program at the Commission. WTA

[11] *Id.* at 206.

[12] *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").

recognizes, however, that financial constraints are not the only barriers that remain to more comprehensive implementation and use of the Framework.

While limited financial resources may be an impediment or challenge, so too is the ability of small businesses, and in this instance small telecommunications carriers in small towns and communities across America, to find and hire employees appropriately trained in cybersecurity. This is a challenge that many in the public and private sectors, including federal, state and local governments, have yet to figure out and which many WTA members identify as a key barrier to improved cybersecurity. It is extremely rare for small telecommunications providers to have sufficient resources to hire dedicated cybersecurity or IT professionals or otherwise designate existing employees to focus solely on cybersecurity issues and assisting with Framework implementation on a full-time basis. Many of WTA's members have expressed concern with their ability to find properly trained cybersecurity professionals in the rural communities they serve. The current demand for cybersecurity professionals with the requisite cybersecurity knowledge and skills far exceeds the available supply,[13] leaving small companies unable to compete in the marketplace for employees with cybersecurity expertise in light of the large salaries these professionals can demand from the national and multi-national corporations. Policymakers and industry must join together to bridge the gap between the supply and demand for cybersecurity professionals, through increased educational initiatives and other efforts, in

[13] *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 Feb. 8, 2016).

order to ensure that today's workforce has the skills and knowledge necessary to address modern cybersecurity challenges.

Small businesses and their existing employees are also in need of education and training regarding cybersecurity and cyber-hygiene. WTA's members have expressed concerns that the lack of knowledge regarding potential threats is a primary challenge in improving cybersecurity risk management practices. Owners of small telecommunications companies that lack full-time employees assigned to cybersecurity-related issues need practical guidance to understand the threats they face and therefore how Framework implementation can help them. Small businesses often 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.

Tools are available to small businesses online through websites of NIST,[14] the Commission[15] and Department of Homeland Security.[16] However, substantially more proactive and coordinated outreach and education efforts are needed to ensure that companies are aware of potential cyber risks and what they can do to combat them, what is expected of them with respect to cybersecurity from a regulatory perspective, and also how they can meet expectations while remaining conscious of budgetary constraints. Coordinated outreach to small businesses on cybersecurity risk management will be critical moving forward, especially as more companies seek to utilize the Framework and increase participation in cyber threat information sharing

[14] *See* National Institute of Standards and Technology, Cybersecurity Framework Industry Resources, *available at* http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm (last accessed Feb. 8, 2016).

[15] *See* Federal Communications Commission, Cyberplanner, *available at* https://www.fcc.gov/cyberplanner (last accessed Feb. 8, 2016).

[16] *See* Department of Homeland Security, U.S. Computer Emergency Readiness Team, Critical Infrastructure Cyber Community Voluntary Program, *available at* https://www.us-cert.gov/ccubedvp (last accessed Feb. 8, 2016).

relationships.[17] For example, NIST and DHS should work directly with sector-specific agencies to conduct trainings regarding Framework implementation. Existing and future outreach efforts need to be better targeted to those that need help the most: small businesses, their employees, and ultimately American consumers.

Furthermore, additional work on development of incentives for implementation of the Framework and other cybersecurity risk management assessment tools and practices is also critical to overcome the financial and practical challenges preventing more widespread use of the Framework. Executive Order 13636 directed the Secretary of the Treasury to identify and recommend incentives that would encourage Framework adoption,[18] however little has been done in recent months with respect to development of incentives. NIST should actively work with industry to develop meaningful incentives that would further voluntary industry Framework adoption and improved cybersecurity risk management practices by addressing cost and other barriers to implementation, such as the provision of technical assistance to small businesses.

III. Conclusion

Since the Framework's release in February 2014, industry has worked toward incorporating the Framework into their cyber risk management efforts, however much work remains particularly for small businesses. As such, the voluntary nature of the Framework remains critical, and NIST should continue to remind regulators that the Framework should not be used as a baseline for developing regulations. Additionally, NIST should provide sufficient

[17] 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.

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

time for industry to digest the Framework and sector-specific guidance before making comprehensive reforms to the Framework. While sector-specific guidance such as the CSRIC IV Report goes a long way toward simplifying the Framework, publication of a variety of illustrative use cases would make the Framework more accessible and useful for companies of all sizes and sectors at this time.

Additionally, substantially more outreach and education efforts are needed before comprehensive changes are made to the Framework in order to ensure that small businesses are not left behind. 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, however the amount of available information can be impossible for small businesses lacking dedicated IT or cybersecurity staffs to wade through. Rather than focusing on additions and updates to the Framework, NIST should work with industry and its other government partners to address the critically important workforce education component of what is necessary to meet 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
400 Seventh Street NW, Suite 406
Washington, DC 20004
(202) 548-0202

By: /s/ Patricia Cave
Patricia Cave
Director of Government Affairs
400 Seventh Street NW, Suite 406
Washington, DC 20004
(202) 548-0202

Dated: February 9, 2016