Before the
U.S. Department of Commerce
National Institute of Standards and Technology

In the Matter of	**)**	**Docket Number**
Developing a Framework	**)**	**130909789-3789-01**
To Improve	**)**	
Critical Infrastructure	**)**	
Cybersecurity		

COMMENTS OF
WTA: ADVOCATES FOR RURAL BROADBAND

WTA, a national trade association comprised of more than 250 rural broadband telecommunications carriers, provides its comments on the Preliminary Cybersecurity Framework proposed by the National Institute of Standards and Technology ("NIST").[1]

WTA's members are primarily very small entities (typical staff: 7 to 15 employees) that serve rural areas that have generally been financially unattractive to and disregarded by larger telecommunications carriers and cable television companies due to their sparse populations, isolated locations, rugged terrain and/or high service costs. Long known as rural telephone companies, WTA members have been deploying broadband facilities and Internet Protocol ("IP") technology during the past decade, and have now evolved primarily into broadband data, voice and video service providers.

WTA and its members are very interested in working with NIST and other entities to help reduce cybersecurity risks to their increasingly broadband networks, and to improve their ability to serve critical infrastructure such as government agencies, power production and distribution companies, hospitals and healthcare facilities, financial institutions, retail distribution centers, and other carriers and Internet service providers.

[1] Improving Critical Infrastructure Cybersecurity Executive Order 13636, Preliminary Cybersecurity Framework, National Institute of Standards and Technology, Oct. 22, 2013.

WTA supports NIST's efforts to avoid developing and imposing a prescriptive regulatory approach to cybersecurity. In addition to maintaining the flexibility to identify and address ever-changing threats, a non-prescriptive approach will allow companies of various types and sizes to tailor their cybersecurity efforts to the resources they possess and the likely threats they face. WTA and its members are particularly interested in the ability to share threat information with other carriers (particularly if sharing protocols are accompanied by appropriate privacy and indemnification provisions), and in the ability to compare and evaluate their cybersecurity efforts against those of similarly situated companies and appropriate industry standards.

At the same time, WTA has concerns that NIST's Proposed Cybersecurity Framework is designed primarily for much larger corporations, and may not be effectively scalable for very small carriers – particularly those with less than twenty (20) [and in many cases, less than ten (10)] employees. WTA members and other small rural companies have little hope of being able to hire or retain experienced cybersecurity professionals and generally lack the resources to allow their small technical and administrative staffs to devote more than a couple hours per week to cybersecurity activities. For example, a small carrier with 2-to-5 somewhat cyber-knowledgeable managers and technicians will drop everything to react to a cyber attack or tangible threat, but does not have the staff resources to engage in extensive cybersecurity meetings, planning and training. Moreover, to make matters worse, WTA members and other rural carriers are presently caught in a financial squeeze wherein they urgently need to invest millions of additional dollars in the infrastructure necessary to extend their broadband facilities and increase their broadband speeds to keep up with the burgeoning broadband demands of their customers, while at the same time Federal Communications Commission ("FCC") universal

service and access "reform" has been limiting or decreasing, as well as rendering unpredictable, two of their three primary revenue streams.

WTA recognizes that NIST, as a non-regulatory standards setting federal agency, does not have the authority to implement many of the policies advocated in these comments. However, WTA believes that due to the nature of this multi-stakeholder Cybersecrity Framework development process, it is an appropriate forum to discuss the cross-jurisdictional issues faced by WTA members and other small carriers in their provision of secure broadband networks and services to rural areas. Without consideration of all of the critical issues facing companies in the implementation of cybersecurity (including the potential financial impediments affecting rural and other small carriers and concerns with the functioning and legal status of future information sharing structures), the effort to develop NIST's Cybersecurity Framework will fail to capture a true picture of the cybsersecurity ecosystem.

WTA and Its Members

WTA is a national trade association that represents more than 250 small telecommunications carriers that provide broadband data, voice and video services and/or traditional voice telephone services in rural portions of the United States. Until recently, WTA's members were predominately incumbent rural local exchange carriers ("RLECs"), also known as rural telephone companies, which primarily furnished voice services. However, since the turn of the century, WTA members have invested significantly in soft switches, fiber optic lines and other broadband infrastructure, and have now evolved to the point where they are preponderantly broadband telecommunications carriers providing increasing amounts of IP and other advanced services.

WTA members are generally very small companies[2] that serve remote and/or rugged rural areas where the per-customer costs of constructing, operating and maintaining both wireline and wireless networks are much higher than in urban and suburban America. Their service areas are comprised mainly of sparsely populated farming and ranching regions; isolated mountain, desert and mining communities; and Native American reservations. Most members serve fewer than 3,000 access lines in the aggregate, and fewer than 500 access lines per exchange.

Even in remote and/or sparsely populated areas, there are critical facilities as well as households and businesses that need to be protected against cybersecurity threats. Virtually every WTA member serves public safety agencies, schools, healthcare facilities and banks whose online operations and records need to be protected. In addition, various WTA member service areas contain critical facilities (such as military bases, power generation and distribution plants, air traffic control facilities, retail distribution centers, and connections for other carriers and Internet service providers) that need to be protected against cyber attacks. To the extent that their resources permit, WTA members have tried to keep informed of likely cybersecurity threats, and of the practices and equipment available to defend against them. Currently, in most cases the operators of critical facilities in the rural service areas of WTA members assume primary responsibility for the firewalls, password systems and other cybersecurity defenses used to protect their facilities. However, if and when problems arise, the local broadband service provider is usually called in to assist with the defense, damage analysis and recovery. Where feasible, some WTA members have installed session border controllers, intrusion detection

[2] Note: the Small Business Administration ("SBA") classifies as "small companies" wireline and wireless telecommunications carriers and resellers having fewer than 1,500 employees. The full-time staffs of WTA members (typically, 7-to-15 employees) are extremely small even for a small company, as is demonstrated by the fact that they comprise only a very small fraction of the SBA's "small company" standard.

systems, firewalls, flow analyzers, anti-virus software and other cybersecurity hardware and software to offer further protection for their networks and customers.

However, as noted above, WTA members' relatively small staffs limit their cybersecurity capabilities. The typical WTA member has 7-to-15 employees, including a manager, a secretary-receptionist, and several customer service representatives, billing and bookkeeping personnel, and plant and installation technicians. Whereas some members may have 20-to-30 employees, others have staffs of only 4-to-6 who perform multiple functions. In light of their very small staffs, WTA members lack the luxury of employing full-time cybersecurity professionals, much less multi-employee cybersecurity departments. Moreover, given that Appendix C of the Preliminary Cybersecurity Framework recognizes that there is a shortage of cybersecurity experts nationwide,[3] most WTA members have little hope of being able to attract and retain cybersecurity professionals. Rather, the typical WTA member has only a couple of employees who have limited experience with cybersecurity matters and who have other responsibilities that prevent them from devoting more than a small fraction of their working hours to cybersecurity. Hence, whereas WTA members can respond on an emergency basis to specific cyber attacks against their networks and customers, they lack the resources 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 training activities.

WTA members are also currently in a major financial squeeze. Whereas they made great strides investing in and deploying broadband infrastructure during the 2000-2008 period, they still have a long way to go to provide their rural customers with the broadband applications and speeds available in urban areas. To date, RLECs have generally upgraded their traditional copper lines to use digital subscriber line ("DSL") technology to provide broadband, and many

[3] Appendix C, p. 37.

have extended fiber optic trunks further and further into their networks in order to increase DSL speeds and provide DSL services to customers located farther and farther from their central offices.[4] However, to provide broadband services and speeds reasonably comparable to those available in urban areas, most individual RLECs are eventually going to need to spend additional millions of dollars to bring fiber optic facilities all the way to the homes or curbs of their rural customers.

Unfortunately, at the very time that substantial additional broadband upgrades are necessary, WTA members and other RLECS have been rocked first by the 2008 financial collapse and then by the Federal Communications Commission's ("FCC's") 2011 order that reduced and limited their critical intercarrier compensation and universal service revenue streams.[5] Put simply, most WTA members rely upon intercarrier compensation and federal universal service support for approximately 50 to 75 percent of their revenue streams.[6] The 2011 FCC "reform" reduces the intercarrier compensation revenue stream of every RLEC by at least 5 percent per year beginning in 2012 toward an ultimate complete phase-out. It also limits the universal service revenue streams of all RLECs, and reduces them for some. A new quantile

[4] Copper DSL lines can provide certain broadband services to customers located about 15,000-to-16,000 feet from a central office. RLECs have been successful in extending DSL service distances and service speeds within their networks by installing fiber lines from their central offices out to pedestals located closer to outlying customer clusters, and then running copper lines from these pedestals to customers that were previously outside the areas where DSL service was available. In other words, RLECs have been replacing their copper telephone and DSL plant with hybrid fiber-copper lines that have significantly increased their DSL service areas and their DSL service speeds.

[5] *In the Matter of Connect America Fund et al.*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket Nos. 10-90, 07-135, 05-37 and 03-109; GN Docket No. 09-51; CC Docket Nos. 01-92 and 96-45; and WT Docket No. 10-208, FCC 11-161, released November 18, 2011.

[6] RLECs vary significantly from each other in size, service areas, network design, costs and revenue streams. Different RLECs rely to different degrees upon intercarrier compensation and universal service support. Typically, intercarrier compensation and federal universal service support each constitute, in different proportions, about 25-to-50% of the revenue streams of various WTA members. More generally, on a macro level, one can think of the typical RLEC revenue stream as consisting of a three-legged stool comprised roughly one-third each of: (1) interstate and intrastate access revenues and other intercarrier compensation; (2) federal and state universal service support; and (3) revenues from local exchange and long distance services provided to residential and business customers.

regression mechanism limits and renders uncertain potential recovery of investments in broadband and cybersecurity facilities, while a revised and expanded cap on corporate operations expense can limit or reduce recovery of recurring increases in cybersecurity and other general administrative expenses. Since 2011, these FCC changes have largely brought to a halt both the availability of financing for, as well as actual RLEC investments in, further broadband upgrades.

WTA and its members urgently desire to resume their advance from the traditional voice telephone business into the emerging broadband world, and to provide the cybersecurity safeguards and other functions that are associated with the provision of broadband services. They are working hard to ease the current financial squeeze, to increase their efficiencies and to develop additional revenue sources. However, until they can improve their financial situation, it is going to be very difficult for WTA members and other RLECS to make the needed broadband network upgrades, as well as to deploy more extensive cybersecurity facilities, functions and personnel.

Important Considerations for Further Development of Cybersecurity Standards

As NIST and its federal partners work with Congress and industry on the development and implementation of cybersecurity standards, it is important that they consider the various challenges faced by small companies like WTA members and other RLECS as described above and fully address the potential hurdles to implementation of sufficient and adaptable cybersecurity protections for RLEC networks that connect various critical operations in rural America. To effectively address these challenges, NIST, Congress, the White House, the Department of Homeland Security (DHS), the FCC and other agencies should first and foremost work to provide financial resources and create financial incentives to enable RLECs and other very small companies to overcome the substantial financial barriers they face when deploying

and implementing the cybersecurity protections needed to address the ever changing nature of cyber threats. NIST should continue its outcome-oriented, non-prescriptive approach to developing a Cybersecurity Framework, but should carefully consider the very different needs, responsibilities and resources of large, mid-sized and small service providers in determining whether and how the ultimate Framework will be relevant, practicable and/or scalable for the various types and sizes of service providers. Additionally, any cyber-threat information sharing program, protocol, or procedure developed by Congress or the Executive Branch to be housed in DHS, NIST, FCC, or another agency, should include a mechanism by which small critical infrastructure operators are able to participate and benefit from such a program, and that protects all participants from legal liability that may result from the sharing and/or receiving of information (particularly, Customer Proprietary Network Information or other personal or proprietary information) in good faith.

Financial Considerations

The most effective method of enabling RLECs and other small service providers to improve their cybersecurity facilities and operations is to provide sufficient financial incentives and support to enable them to obtain the necessary equipment, staff and training. While in an ideal world every broadband network would be protected effectively from cyber attacks, the high costs associated with such blanket security exceed the resources of most RLECs and other small service providers. For many RLECs, this presents an unfortunate double bind wherein they may be forced to choose between making the investments necessary to upgrade their broadband facilities and service and making the investments and expenditures necessary to improve their cybersecurity facilities and operations.

DHS has proposed several possible incentives, including rate increase allowances for regulated industries.[7] For RLECs that are experiencing continuing line losses for various demographic and economic reasons and that are already required by the FCC to increase their monthly rates several times during the foreseeable future, additional rate increases are a recipe for additional and potentially crippling potential line losses and customer revenue decreases. Unfortunately, telecommunications services are far more price sensitive than other utilities such as electricity and water. If RLECs were to raise their monthly service rates significantly to recover the costs of new or enhanced cybersecurity protections, at least some consumers would be likely to cancel their service, thereby undermining financial support for both broadband expansion and cybersecurity.

An alternative incentive proposed by DHS is to give grants to entities seeking to upgrade their cybersecurity capabilities. WTA finds this idea interesting, so long as such grants would not draw resources away from existing grant or loan programs supporting broadband upgrades. Additionally, a grant model would need to recognize that the terms and conditions of such grants must remain sufficiently flexible to allow recipients to adapt to evolving cyber threats.

Ultimately, the most effective way to reduce the financial barriers that RLECs face in adopting improved cyber defenses would be to modify the high-cost mechanisms of the FCC's Universal Service Fund to recover increased cybersecurity costs without offsetting reductions to other elements of high-cost support. Cybersecurity is a new and expensive function originating with the evolution to an IP and broadband world. Further, cybersecurity facilities and procedures are an important and valuable protection for consumers. Because cybersecurity concerns and costs will have arisen largely after the 2011 baseline year on which the FCC's high-cost support

[7] Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, DHS Incentives Study: Preliminary Analysis and Findings, Department of Homeland Security, June 21, 2013.

mechanisms and budgets are based, cybersecurity costs should be recoverable from the existing FCC high-cost support mechanisms but should not be subject to or trigger the regression caps or corporate operations expense caps that reduce or limit the high-cost support of some RLECs. For example, the FCC could be urged to adopt a streamlined waiver process that would eliminate or reduce the capping of an RLEC's high-cost support if the RLEC could show that new and reasonable cybersecurity investments and/or new and reasonable cybersecurity operating expenses were the cause of all or a specified portion of its relevant expenses that exceeded the subject cap.

Flexibility and Scalability for Small Companies

WTA commends NIST's focus on creating an outcome based, non-prescriptive cybersecurity framework. Such an approach is important to enable small companies to have the necessary flexibility in implementing cybersecurity according to the nature and size of their business and the degree of their cyber-risk. NIST's cybersecurity framework should continue to be flexible enough to allow experimentation and the use of other industry-specific cybersecurity standards such as those developed by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC). NIST should continue this approach and work with other federal agencies to ensure that they adhere to the same principles. Federal regulators should ensure that the lack of adoption of a specific level or specific set of cybersecurity preparations as described by NIST's cybersecurity tier-based framework cannot be used by private entities to skirt existing regulatory responsibilities such as network interconnection. Additionally, it should be made clear that NIST's Cybersecurity Framework is one of many cybersecurity standards available for businesses and that it should not become the *de facto* legal standard by which companies are judged when faced with a legal inquiry for a potential cyber-breach.

WTA has concerns whether NIST's Cybersecurity Framework will be effectively scalable with respect to small companies, and, if so, how such scalability will be implemented. As presently described, it appears that the Cybersecurity Framework is predominately designed for large companies with substantial cybersecurity departments or task forces. As discussed above, WTA's RLEC members have very small staffs and very limited financial and other resources that can be dedicated to cybersecurity efforts. Hence, in the next iteration, it would be very helpful if NIST could provide some examples of how the Framework could be scaled down to provide effective procedures and assistance for the hundreds of RLECs and other very small service providers that need to address cybersecurity issues. WTA agrees with NIST's intention to continuously evolve its cybersecurity framework as implementation occurs and practical realities dictate. However, it may be worth conducting small scale testing on various forms and sizes of infrastructure operators prior to the release of the Framework to ensure that the recommendations do not result in wasteful or ineffective initiatives that are designed primarily for large companies.

Information Sharing

Information sharing is a crucial component of any future cybersecurity framework. While NIST's framework does not address such an arrangement, it is critical to envision how a legislatively enabled cyber-threat information-sharing program would function in relation to currently existing or developing cybersecurity standards. Of principle concern to RLECs is that any such information-sharing program should be accompanied by liability and indemnification protections for information shared, received, or acted upon in good faith if that information or the actions resulting from receiving the information accidentally affects an innocent party. This is particularly critical due to the statutory and regulatory restrictions placed upon the use of

Customer Proprietary Network Information ("CPNI") by common carriers, as well as the statutory and common law protection of private personal information and proprietary business information regularly transported over broadband networks. RLECs and other carriers simply cannot afford to share, receive or act upon information in response to actual or alleged cybersecurity threats if doing so can expose them and their employees to substantial potential criminal or civil liability. Additionally, participation in a government-coordinated information-sharing program should be voluntary in order to avoid unmanageable expenses for companies already struggling to afford their own cybersecurity initiatives. All information shared as part of this program should remain confidential including information about a company's business operations, cybersecurity preparations, or a specific cyber-event. Such confidentiality is necessary to avoid concerns related to or that provide disincentives to a company that wishes to participate, but does not wish to risk exposing themselves to negative publicity. Finally, since there are advantageous network effects of an information-sharing program where many entities participate to the extent they are practically and financially able, the program should include mechanisms through which small companies with fewer resources are able to participate and benefit from shared cyber-threat information without requiring reciprocal information sharing agreements or burdensome payments.

Conclusion

WTA applauds NIST's flexible and non-prescriptive efforts to develop a Cybersecurity Framework. It hopes to work with NIST and other agencies to develop cybersecurity guidelines that are scalable or otherwise practicable for RLECs and other very small companies, and that adequately consider and effectively address the limited staff and financial resources of WTA

members and other RLECs, and their concerns about information sharing, the protection of privacy and proprietary information, and indemnification from lawsuits and legal liability.