Before the
National Telecommunications Information Administration
Washington, D.C. 20230

In the Matter of	)	
	)	
Incentives To Adopt Improved Cybersecurity Practices	)	Docket No. 130206115-3115-01
	)	

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association[1] ("NTCA") hereby submits these comments in response to the National Telecommunications Information Administration ("NTIA") Notice of Inquiry ("NOI") on incentives designed to promote participation in a voluntary program to be established by the Department of Homeland Security ("DHS") regarding the cybersecurity framework being developed by the National Institute for Standards and Technology ("NIST").[2] NTCA applauds the federal government's efforts to encourage participation in voluntary cybersecurity best practices, such as information sharing about network cyber attacks and intrusions. Consistent with Executive Order 13636,[3] however, any cybersecurity framework must be voluntary. The government should not adopt "incentives" that effectively turn a voluntary cybersecurity framework into a new unfunded mandate on the communications industry. Instead, the government should establish confidentiality and liability protections that could promote continued information sharing about cyber attacks and threats.

[1] All of NTCA's members are full service local exchange carriers ("LECs") 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] Incentives to Adopt Improved Cybersecurity Practices, Notice of Inquiry, Docket No. 130206115-3115-01, 78 Fed. Reg. 18954 (Mar. 28, 2013).

[3] Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

INTRODUCTION

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 areas of the country that large companies will not serve. Rural telecom providers are a critical link in the nation's telecommunications network, serving forty percent of America's landmass and five to seven percent of its population.

Unlike most other "critical infrastructure" industries, competitive forces across the communications industry help to create market incentives to ensure that networks are adequately protected from cyber threats. Moreover, as small businesses based in the communities they serve, rural telecom providers have strong incentives to ensure the security of their network users. Indeed, rural telecom providers are experts at serving the needs of their customers, have implemented adequate and successful cyber defense strategies, and continue to modify these strategies to meet the unique needs of their customers.

The communications industry long ago established numerous best practices to detect and prevent cyber threats, and the industry continues to revise these best practices as the threats evolve. These best practices should form the basis for any voluntary cybersecurity framework for the communications sector. The competitive forces at play in the communications industry will ensure that industry follows cybersecurity best practices – as it does today – and additional incentives to adopt new best practices are largely unnecessary. Nevertheless, the federal government can assist industry's cybersecurity efforts by establishing clear liability protections for telecom providers that engage in information sharing to prevent cyber attacks.

Consistent with Executive Order 13636,[4] any cybersecurity best practices must be voluntary. The government should not adopt incentives that effectively turn a voluntary cybersecurity framework into a new unfunded mandate on the communications industry.

I. MARKET FORCES WILL CREATE INCENTIVES TO ADOPT AN EFFECTIVE CYBERSECURITY FRAMEWORK.

Market forces obviate the need to impose a cybersecurity framework on the communications industry. Comprehensive cybersecurity best practices already have been developed for the industry.

Unlike other critical infrastructure providers, competitive forces across the communications industry help to create market incentives to ensure that providers adequately protect their networks from cyber threats. Indeed, the President's National Security Telecommunications Advisory Committee ("NSTAC") has concluded that "market incentives will remain the fundamental driver of industry practices and standards [and] companies will continue to offer services that are as resilient and secure as customers' preferences dictate."[5]

The market forces that NSTAC identified have long pushed the communications industry to address network reliability and cybersecurity. More than twenty years ago, the Federal Communications Commission ("FCC") chartered the Network Reliability Council ("NRC") to establish best practices to ensure network resiliency and reliability.[6] In 2001, NRC's successor, the Network Reliability and Interoperability Council ("NRIC"), was directed to "assess

[4] Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

[5] NSTAC, NSTAC REPORT TO THE PRESIDENT ON COMMUNICATIONS RESILIENCY 14 (2011) ("NSTAC Report") *available at* http://www.ncs.gov/nstac/reports/NSTAC Report to the President on Communications Resiliency (2011-04-19)(Final)(pdf).pdf.

[6] For a brief history of the NRC, *see http://www.nric.org/pubs.*

vulnerabilities in the public telecommunications networks and the Internet and determine how best to address those vulnerabilities to prevent disruptions that would otherwise result from terrorist activities, natural disasters, or similar types of occurrences."[7] The best practices NRC and NRIC adopted have been revised as threats have evolved.

The Communications, Security, Reliability, and Interoperability Council ("CSRIC") – the successor to NRIC – continues to work on cyber best practices.[8] In March 2011, a CSRIC working group comprehensively reviewed all cybersecurity-related best practices[9] and recommended approximately 400 new or modified cybersecurity best practices.[10] CSRIC remains committed to this issue and is continuing its cybersecurity best practices efforts.

NTCA members have implemented these cybersecurity best practices to the extent applicable to their businesses. Based largely in the communities they serve, America's small rural communications providers have always displayed a strong commitment to responding effectively to the interests and needs of consumers, while simultaneously planning for, and appropriately reacting to, both potential and actual emergencies and threats involving their infrastructure and services.

The adoption of new, different, voluntary best practices by the federal government likely will create needless confusion and potentially conflict with existing industry best practices. Thus, rather than develop a new cybersecurity framework for the communications industry and

[7] NRIC VI Charter *available at* http://transition.fcc.gov/hspc/NRIC_recharter.pdf.

[8] *See* CSRIC III Charter *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC%20Charter%20Renewal%202011%20FINAL.pdf (CSRIC IV is currently being formed). NTCA has actively participated on this Council in the past.

[9] *See* CSRIC Working Group 2A, Cyber Security Best Practices, Final Report at 3 (Mar. 2011).

[10] *Id.* at 7.

incentives to promote adoption of this new framework, the administration should utilize the existing cybersecurity best practices that NRIC and CSRIC already have established.[11]

Managing cybersecurity risk is critical to the success of a rural telco's business. In order to be successful and retain the confidence of its subscriber base, the rural telco must maintain a secure network capable of transmitting and receiving sensitive and personal data and information. Precise security measures and practices are based upon the individual needs of the service provider's customers. For instance, if a rural telco services defense contractors or military facilities, its network security procedures will likely be very different from those of a telecom provider that services a small agricultural community. Rural telcos must be able to retain this regulatory flexibility to meet the needs of their unique customer bases and the wide disparities in the areas they serve.

Both CSRIC and NRIC recognized that every best practice may not "be appropriate for every company in every circumstance."[12] Consistent with this finding, the federal government should avoid adopting any incentives that are tied to adoption of *every* cyber best practice ultimately incorporated into the NIST cybersecurity framework. A service provider should be expected to implement only those best practices that align with the individual risk encountered by the provider and its specific customers. Any incentives also should ensure that smaller providers are not penalized for failing to implement certain best practices that would provide little benefit compared to the cost of implementation.

[11] Each of the relevant FCC advisory groups – NRC, NRIC, and CSRIC – included communications carriers, equipment manufacturers, and regulators who voluntarily served in order to establish best practices to ensure network reliability and to combat threats to homeland security.

[12] *See* CSRIC Working Group 2A, Cyber Security Best Practices, Final Report at 3 (Mar. 2011).

As small businesses, rural telecom providers must assess the costs and benefits of enhancing their cybersecurity, balancing security risk against financial resources and the usability of the network. NTCA's members perform routine risk assessments, determining each broadband service provider's qualitative and quantitative risk, the probability that an incident will occur, and its ability to minimize the likelihood of network attack or disruption. Based upon the needs and vulnerabilities of their various networks and their customers, NTCA's members are deploying all manner of cyber defenses. Rural providers are experts at doing a lot with little, and many already employ personnel with cyber expertise who handle other duties as well.

II. THE GOVERNMENT SHOULD REFRAIN FROM ESTABLISHING UNFUNDED MANDATES

The federal government should refrain from adopting "incentives" that effectively establish new unfunded mandates on the rural telecom industry. The imposition of penalties against companies that elect not to follow some (or all) of the proposed cybersecurity framework would effectively force participation and become an unfunded mandate.

Rural telecom providers have limited resources, as they rely on the Universal Service Fund ("USF"), intercarrier compensation ("ICC"), and U.S. Department of Agriculture Rural Utilities Service ("RUS") and other loans to accomplish their service mission. Although they have an admirable track record of efficiently leveraging every resource available to them, rural rate-of-return telecom providers are facing comprehensive FCC reforms which drastically affect their traditional USF and ICC cost-recovery revenue streams, and as a byproduct, tight credit markets which restrict a telco's access to operating capital. Any new unfunded regulatory mandates – whether in the form of traditional regulations or a punititive incentive regime –

could add another level of uncertainty to the marketplace and divert already strained resources from important projects, such as broadband deployment and adoption efforts.

III. THE ADOPTION OF CERTAIN INCENTIVES COULD ENCOURAGE INFORMATION SHARING

A. Carriers Sharing Information Regarding Cyber Attacks, Damage, or Threats Should be Entitled to Liability Protection

NTCA members fully support the goals of Executive Order 13636, which directs relevant federal agencies to increase the "volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities," such as communications service providers, "so that these entities may better protect and defend themselves against cyber threats."[13] Current laws limit providers' ability to share threat information with the government and other private sector entities, however. The administration therefore should seek a legislative fix that would (1) define clearly the categories of information that providers can share with the government for cyber security purposes, and (2) immunize providers from liability for sharing such information with the government for purposes of preventing and detecting cyber threats.

The Electronic Communications Privacy Act ("ECPA") demonstrates why a legislative fix is necessary. ECPA allows providers to monitor communications to protect their own networks, but it prohibits providers from voluntarily sharing this information (absent customers' consent) with the government, unless necessary to the "protection of the rights or property of the provider of that service" or the provider, in good faith, believes an emergency involving danger of death or serious physical injury requires disclosure without delay.[14] Thus, ECPA does not

[13] Executive Order 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

[14] 18 U.S.C. § 2702(b)(5), (b)(8).

expressly authorize providers to intercept communications in order to protect subscribers' property. Communications providers need immunity to ensure they are not held liable for good-faith efforts to protect subscribers' property.

Moreover, ECPA arguably prohibits providers from voluntarily sharing certain cyber information unless it falls within the limited exemptions. There currently is no exemption that could cover the routine sharing of cyber threat information envisioned by the government.

Finally, antitrust laws, which limit information sharing between certain companies to prevent anticompetitive activities, can discourage providers from sharing information with other private sector entities. Congress should establish a safe harbor to protect companies from liability under these laws when they share threat information with other providers for cybersecurity purposes.

B. It Should Be Illegal to Publicly Disclose Cybersecurity Information or to Use Such Information to Gain a Competitive Advantage

To ensure that communications carriers share information about outages and cyber threats, any cybersecurity framework should make clear that information voluntarily supplied to combat cyber threats is confidential and cannot be used competitively by recipients of the information. Many communications carriers currently share information regarding network outages and threats,[15] but this cooperative environment depends upon the non-disclosure of the shared

[15] As DHS has noted:

> The communications companies that own, operate, and supply the Nation's communications infrastructure have historically factored natural disasters and accidental disruptions into network resiliency architecture, business continuity plans, and disaster recovery strategies. The interconnected and interdependent nature of these service provider networks has fostered crucial information sharing and cooperative response and recovery relationships for decades.

DHS, COMMUNICATIONS: CRITICAL INFRASTRUCTURE AND KEY RESOURCES; SECTOR SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN at 2 (2007) ("DHS Report") *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf.

information. In fact, the FCC's entire network outage reporting system currently is premised upon confidentiality, and this common-sense approach should be replicated in a cybersecurity framework. According to the FCC, "[g]iven the competitive nature of many segments of the communications industry and the importance that outage information may have on the selection of a service provider or manufacturer, we conclude that there is a presumptive likelihood of substantial competitive harm from disclosure of information in outage reports."[16] Thus, absent clarity that information shared as part of the new cybersecurity framework will be treated confidentially, communications providers may no longer share information as they do today. Further, the federal government should consider using the National Cybersecurity Communications Integration Center ("NCIC") as the information sharing clearinghouse, allowing information to be shared anonymously and thereby minimizing the competitive use threat. NCIC was established by the Office of Cybersecurity and Communications at the Department of Homeland Security and its continuing mission is it in operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, performing cutting edge analysis, sharing actionable and comprehensive information in real time, and ensuring a whole-of-nation approach to response, mitigation, and recovery efforts.

CONCLUSION

NTCA members recognize the importance of securing our nation's critical infrastructure and appreciate the development of risk-based standards that will provide

[16] New Part 4 of the Commission's Rules Concerning Disruptions to Communications, Report and Order, 19 FCC Rcd 16830, 16855 (2004).

industry benchmarks and suggested guidelines. While it is essential that the public and private sectors work together to secure American's critical infrastructure, the federal government should refrain from effectively establishing any new unfunded regulatory mandates on the rural broadband industry. Moreover, given the well-developed cybersecurity best practices that already exist for the communications industry, the adoption of any new cybersecurity best practices for the industry likely will create needless confusion. Further, mandated compliance with any new cybersecurity framework would divert already-strained resources from important projects, such as broadband adoption and deployment in rural areas. The federal government should instead focus on instituting clear liability protection for telecom providers that share information to prevent attacks or damage and protecting such information from public disclosure.

Respectfully submitted,

By: /s/ Jill Canfield
Jill Canfield
Director – Legal & Industry

/s/Jesse Ward
Jesse Ward
Industry & Policy Analysis Manager

4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203
jcanfield@ntca.org
703-351-2000 (Tel)
703-351-2036 (Fax)