Before the
National Telecommunications Information Administration,
U.S. Department of Commerce
Washington, D.C. 20230

In the Matter of	)	
	)	
Promoting Stakeholder Action Against	)	Docket No.
Botnets and Other Automated Threats;	)	180103005–8005–01
Notice, Request for Public Comment	)	

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION & SUMMARY

NTCA–The Rural Broadband Association[1] ("NTCA") hereby submits these comments in response to the National Telecommunications Information Administration ("NTIA") Request for Comment on a draft Report[2] about actions to address automated and distributed threats to the digital ecosystem as part of the activity directed by Executive Order 13800, ''Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.''[3]

NTCA represents more than 850 rural rate-of-return regulated telecommunications providers. NTCA's members help put rural Americans on an equal footing with their urban

[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] "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," Draft for Public Comment, Transmitted by The Secretary of Commerce and The Secretary of Homeland Security, rel. January 5, 2018, available at: https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf ("Draft Report").

[3] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," rel. May 11, 2017, available at: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

neighbors by providing broadband and other telecom services in remote and rural areas of the country often underserved by larger operators. Rural telecom providers are a critical link in the nation's telecommunications network, serving approximately 37% of America's landmass and 5% of its population.

NTCA appreciates the federal government's efforts to address automated and distributed threats. The draft Report, for the most part, correctly acknowledges that botnets and related threats are an ecosystem-wide challenge, which cannot be resolved without the assistance and support of many participants, both within the United States and abroad. Indeed, Internet service providers ("ISPs") alone cannot mitigate botnets attacks; rather, it will require the cooperation of a variety of stakeholders including consumers, enterprises, and other technology infrastructure suppliers such as hardware manufacturers; system integrators; content delivery networks; and software, cloud and edge-services providers, to name a few.[4]

Given this, NTCA's comments are focused on the efficacy of specific, proposed action items and supporting statements. In particular, Action 4.3, which seeks to foster sector-specific regulatory requirements, is inconsistent with the draft Report's macro-level supporting findings discussed within the Current Status of the Ecosystem. NTIA correctly asserts that static, prescriptive regulation is, by its very nature, backward-looking and it cannot keep pace with the quickly evolving threat landscape—but this assertion stands in direct opposition to its recommendation calling for new regulatory mandates to address botnets and related cyber threats. Further, rural telecommunications providers already deploy cyber defenses according to

[4] *See* "Industry Technical White Paper," Communications Sector Coordinating Council, rel. July 17, 2017, available at: https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

their needs and vulnerabilities. To address botnets and related distributed attacks, small ISPs have adopted a variety of industry best practices highlighted throughout the draft Report, consistent with their individual company's capabilities, resources, and underlying risk tolerance. And any new unfunded regulatory mandates could add another level of uncertainty to the marketplace and divert already strained resources from important projects, such as broadband deployment and adoption efforts or maintenance of service reliability. Given these concerns and the limitations of the approach stated in Action 4.3, NTIA should decline to formalize the recommendation.

As an alternative, industry best practices are best suited to address the evolving threat landscape. Indeed, NTIA has included several actions which seek to develop and promote the use of industry best practices, such as those within recommended Action 2.5 and Goal 5. However, industry best practices should be voluntary, flexible, scalable, and risk-based, consistent with a risk-management approach to cyber threats—the foundation of Executive Order 13800. NTCA urges NTIA to revisit its draft Report to ensure its recommended goals and actions are consistent with these guiding precepts.

Finally, NTCA agrees that "automated, distributed attacks are a global problem"[5] and, therefore, any approach to mitigate botnets will only prove successful if there is an international, coordinated effort. NTIA has appropriately identified this limitation within the Report; however, its recommended Goals and Actions are overwhelmingly focused on U.S.-based companies and providers. NTIA should review the draft Report to ensure its roadmap for future Goals and Actions emphasizes international cooperation and coordination.

[5] Draft Report, page 7, Principle Themes.

II. NTIA SHOULD DECLINE TO FINALIZE ACTION 4.3, WHICH SEEKS TO ADOPT SECTOR-SPECIFIC REGULATORY REQUIREMENTS

The federal government should refrain from establishing any new unfunded mandates on the rural telecom industry as static, prescriptive regulation cannot effectively address botnets and related distributed threats.

A. Static, Prescriptive Regulations Cannot Keep Pace with Evolving Threats

Within the draft Report, NTIA acknowledges the limitations of a static set of regulations to address botnets and other related distributed and automated attacks. NTCA agrees that "[d]ue to the complexity and diversity across the IoT [internet of things] landscape, it is difficult to envision a set of one-size-fits-all rules that could ensure security while keeping pace with the rate of change and the dynamic nature of the threat environment."[6] Static, prescriptive regulation is, by its very nature backward-looking, and it cannot effectively mitigate quickly evolving threats. Unfortunately, this macro-level finding is inconsistent with proposed Action 4.3 which seeks to engage "[r]egulatory agencies…to foster sector-specific security requirements."[7] NTCA disagrees with the regulatory nature of the recommendation. As NTIA itself has stated, "[c]ompliance requirements, or mandating specific regulations, may address some risks, but often carry with them a greater burden while still leaving the broader ecosystem insecure."

Given these limitations, NTIA should remove any reference to the creation of a traditional, prescriptive regulatory requirements to address botnets and distributed cyber threats. Instead, as discussed further below, the federal government should seek to encourage industry to develop and document best practices and promote their awareness and use.

---

[6] *Id.*, page 34, Action 4.3.

[7] *Id.*

B. Rural Telecommunications Providers are Experts at Deploying Cyber Defenses Consistent With their Needs and Vulnerabilities

Cybersecurity mandates are unnecessary to encourage rural broadband service providers to meet the needs of their customers. Managing cybersecurity risk is critical to the success of a rural telco's business. To 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.

NTCA's members perform routine risk assessments, determining the qualitative and quantitative risk to their networks, the probability that the threat will occur, and the provider's 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, and NTCA is encouraging and assisting them with this effort.[8] Rural providers are experts at doing a lot with little, and many already employ personnel with cyber expertise who handle other duties as well.

More specifically, to address botnets and related automated and distributed attacks, small telecom providers have implemented various industry best practices. For instance, to restrict

[8] NTCA has engaged in a comprehensive outreach and education campaign to alert its members to the Framework and the key attributes of a risk-management cybersecurity program. In 2016 alone, more than 2,000 attendees participated in a dozen NTCA-led events around the country. And in 2017, NTCA's Cybersecurity Summit and related online and in-person cybersecurity educational events drew more than 1,500 attendees. In addition, NTCA recently entered into a partnership with the Department of Homeland Security (DHS) and National Institute for Hometown Security (NIHS) to provide operators of small, rural telecommunications networks with robust educational programming and insights into industry best practices to aid their development of more comprehensive cybersecurity risk-management programs. The association's new cybersecurity education program, named NTCA CyberWise, is supported by an award through the DHS National Infrastructure Protection Plan Security and Resilience Challenge and the Office of Infrastructure Protection, in partnership with NIHS. The challenge provides opportunities for the critical infrastructure community to help develop technology, tools, processes, and methods that address immediate needs and strengthen the long-term security and resilience of critical infrastructure.

malicious traffic from traversing their networks, small ISPs may implement network filtering techniques such as Access Control Lists ("ACLs"), and ingress and egress filtering to limit distributed denial of service ("DDOS") attacks which leverage spoofed IP addresses. In addition, to the extent it is practical, some small ISPs have invested in commercial anti-denial of service ("DOS") services to mitigate attacks, often pooling their resources to purchase the service on a regional or statewide basis. However, it should be noted that commercial anti-DOS products have limitations; in the worst-case scenario, they may trigger a false positive alert that could inadvertently cause a denial of service attack that attempts to block legitimate traffic. For instance, many anti-DoS products function by detecting abnormally large amounts of a specific type of traffic. However, if a customer turns up a new Internet based service that is improperly configured, the anti-DOS service may block this never-before-seen large amount of traffic.

Specific implementation of network security best practices is an individual company decision; there will be necessary variation depending upon a company's resources, capabilities, and technical sophistication, and consistent with its risk profile and tolerance. 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. Small, 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.

To be clear, small ISPs understand their responsibility for protecting their networks and customers by implementing cost-effective industry best practices; it is a duty that that they do not take lightly. Small ISPs are holistically assessing addressing cyber threats to critical infrastructure and core services. In addition, to further protect the network edge, many rural telcos are now providing customers with managed Wi-Fi routers and anti-virus services to

increase security in residential homes and businesses. Despite these advancements, small, rural telecom providers should not be held to the same standard as their much larger ISP counterparts which operate with a corresponding exponential increase in resources. Indeed, as documented in several related proceedings, small telecom providers have extremely limited financial, technical, and operational resources,[9] and these constraints must be considered when the federal government seeks to review the requirements of ecosystem participants. Under the current regulatory environment, small, rural ISPs are able to cost effectively and efficiently adopt industry best practices to address evolving market-based threats.

C. Any New Unfunded Regulations Might Inadvertently Deter Resources from Other Critical Projects

To the extent that they have already put into place sufficient security protections to meet their individual residential customers' and businesses' needs, the government should refrain from then placing additional mandates that defer resources from other critical projects. As previously noted, NTCA's members are small service providers that have limited resources. Although they have an admirable track record of efficiently leveraging every resource available to them, rural broadband providers face unique challenges associated with deploying and operating communications networks in areas characterized by low population density, often in remote locations, that result in dramatically higher per-customer costs. Any new unnecessary, unfunded

[9] This is well documented in various proceedings, including the Federal Communications Commission "Communications Security, Reliability and Interoperability Council IV Working Group 4 Report on Cybersecurity Risk Management and Best Practices," at 204, 206, and 391: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf. *Also see* Comments of NTCA, *In the Matter of Incentives to Adopt Improved Cybersecurity Practices*, NTIA, Notice of Inquiry, Docket No. 130206115-3115-01, 78 Fed. Reg. 18954, Nov. 21, 2012, at 6; Comments of NTCA, *In the Matter of Request for Comments; Draft 2 of Version 1.1 of the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, NIST, Jan. 19, 2018.

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

III. NTIA SHOULD PROMOTE THE USE OF INDUSTRY-DRIVEN BEST PRACTICES, WHICH ARE VOLUNTARY, FLEXIBLE, SCALABLE AND RISK-BASED, CONSISTENT WITH EXECUTIVE ORDER 13800

Industry best practices are best suited to address the evolving threat landscape, capable of adapting quickly and effectively to meet market-based risks. Within the draft Report, NTIA acknowledges that industry best practices are an effective solution to address botnets and other related automated and distributed threats.[10] Indeed, NTIA has included several Action items which seek to develop and promote the use of industry best practices, such as within recommended Action 2.5 and Goal 5. This approach is consistent with the Federal government's longstanding commitment to a public-private partnership approach to address security.[11] NTCA applauds these recommendations. To assist small telecom providers, NTCA will continue to provide opportunities for small providers to share best practices, including network protection, detection, and response strategies.

However, industry best practices are voluntary, flexible, scalable, and risk-based, consistent with a risk-management approach to cyber threats—the foundation of Executive Order

[10] Within the draft Report, many of the recommended Actions refer to the development and/or promotion of best practices, including Action 1.2, 1.4, 2.5, and 4.2.

[11] The public-private partnership for critical infrastructure protection and cybersecurity has a long, evolutionary history. Government and industry collectively created and fostered this approach, which has culminated today in the National Infrastructure Protection Plan ("NIPP"), a shared vision and blueprint which guides the national effort to manage risk to critical infrastructure. For more, see the "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," Department of Homeland Security, available at: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

13800. NTCA urges NTIA to revisit its draft Report to ensure all its recommended goals and actions are consistent with these guiding precepts. For instance, Action 2.5 states, "The federal government should work with U.S. and global infrastructure providers to expand best practices on network traffic management across the ecosystem." This effort should seek to develop a range of best practices for ecosystem participants to select from and implement consistent with their network vulnerabilities, capabilities, and individual risk tolerances.

Finally, NTCA agrees that "automated, distributed attacks are a global problem"[12] and, therefore, any approach to mitigate botnets will only prove successful if there is an international, coordinated effort. NTIA has appropriately identified this limitation within the draft; however, its recommended Goals and Actions are primarily focused on U.S.-based companies and providers. Rather, the federal government should seek to encourage meaningful international engagement and commitment to adopting best practices on a global basis.

[12] Draft Report at page 7, Principle Themes.

IV. CONCLUSION

NTCA members recognize the importance of securing our nation's critical infrastructure and appreciate the development of risk-based standards that will provide industry benchmarks and suggested guidelines. While it is essential that the public and private sectors work together on securing American's critical infrastructure, the federal government should refrain from establishing any new unfunded regulatory mandates on the rural telecom industry. The federal government should instead focus its efforts on supporting the industry-led development and promotion of awareness best practices within the United States and abroad.

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)

February 12, 2018