Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90

COMMENTS
OF
WTA – ADVOCATES FOR RURAL BROADBAND

WTA - Advocates for Rural Broadband ("WTA") hereby submits its Comments in response to the Commission's *Notice of Inquiry*, FCC 22-18, released February 28, 2022, in the captioned proceeding ("*NOI*").

WTA is a national trade association that represents more than 360 rural local telecommunications carriers ("RLECs") that provide voice, broadband and other services to some of the most rural, remote, rugged, sparsely populated, and expensive-to-serve areas of the United States. WTA members have constructed and operated rural voice and broadband networks – often as providers of last resort – in high-cost farming, ranching, mining, mountain, forest and desert areas, as well as on Native American reservations and other Tribal Lands. The typical WTA member serves fewer than 5,000 customers per service area and has fewer than 50 employees.

WTA members are familiar with cybersecurity concerns and dangers, and strive to do their part in protecting the nation and their customers against cyberattacks and frauds. However, they have limited financial and personnel resources with which to defend against sophisticated and constantly changing probes and attacks by both state-backed and non-state entities.

Role of the Commission

WTA believes that the Commission's most effective and efficient role in cybersecurity matters would be to advise voice and broadband service providers of available cybersecurity

resources and to warn them of the current tactics being employed by entities engaging in cyberwarfare and cybercriminal activities that specifically threaten the reliability and resiliency of the nation's communication infrastructure. Given the constantly changing ploys used in cyberattacks, such up-to-date information is essential in guarding against security breaches.

In addition, the Commission can and should work with other federal agencies – including the Cybersecurity and Infrastructure Security Agency ("CISA"), the Department of Homeland Security ("DHS"), the National Institute of Standards and Technology ("NIST"), the Federal Bureau of Investigation ("FBI") and the National Security Agency ("NSA") – to provide advice and recommendations to service providers with respect to cybersecurity equipment, practices, threats and counter-measures.

However, the Commission should not adopt regulations that require service providers to implement specific cybersecurity technologies, equipment or practices. Such specific regulation is not likely to achieve regulatory clarity because it unfortunately operates far too slowly to reliably and materially assist in the prevention or minimization of changing modes of cyberattack. During the time that it takes for the Commission to prepare a notice of proposed rulemaking, accept and review comments and reply comments, draft and adopt an order, and wait for such order to become effective after Federal Register publication, the technical or procedural requirements adopted by the Commission therein are likely to have been long superseded and rendered inadequate by evolving cyberattack strategies and tactics.

WTA notes that detailed technical and procedural requirements are rendered further problematical by the fact that Border Gateway Protocol ("BGP") routing security is an international problem. Even if service providers in the United States are able to spend massive sums to acquire the hardware, software and personnel to secure BGP routing, that may still not

protect the United States from harmful and malicious routing hijacks that originate in other countries (whether friendly or unfriendly, and whether the attackers are government agents or non-government entities).

To the extent that the Commission elects to become involved in more detailed cybersecurity policies and practices, WTA believes that BGP security and other cybersecurity functions would be much more effectively and efficiently performed by Tier 1 and Tier 2 networks rather than by RLECs and other small service providers. The Commission should require Tier 1 and Tier 2 networks that peer directly with RLECs and other Tier 3 service providers for internal connectivity to implement certain cybersecurity controls and protections for BGP security between peering partners, including at the Internet Exchange Points ("IXPs") through which traffic to and from RLECs and other small service providers must pass.

The major cybersecurity problem faced by many RLECs and other small service providers is that they have a very difficult time recruiting and retaining qualified cybersecurity personnel. Given the growing need for cybersecurity professionals and the resulting opportunities and salaries with larger companies and in more urban areas, it is increasingly difficult for small rural service providers to hire experienced cybersecurity professionals as well as to retain in-house employees if and when they are able to train them in cybersecurity matters. At a time when WTA members and other RLECs are focusing their limited resources on providing higher speed broadband services to more of their customers and extending service into unserved and underserved areas, the growing expenses of cybersecurity hardware and software, cybersecurity consultants and cybersecurity insurance are placing greater strains on our members. And even if they make substantial cybersecurity investments, some RLECs and other small providers may still lack employees with sufficient expertise to recognize and respond rapidly to a cyberattack. Hence, to

the extent that BGP routing cybersecurity can be effectively provided at the Tier 1 and Tier 2 network levels, it may be much more efficient for the Commission to encourage the concentration of most or all BGP routing cybersecurity responsibilities, resources and spending at those levels.

Specific Border Gateway Protocol Issues

WTA members – like all RLECs – range in size from small companies that have BGP routers and experienced cybersecurity staffs to much smaller companies that lack a BGP router and/or an employee with cybersecurity expertise. As a result, there is no "one size fits all" solution for WTA members.

For those WTA members that have invested in BGP equipment and cybersecurity resources, the question generally comes down to whether additional cybersecurity investment provides enough additional protection to be justified. For example, some WTA members have found that the free version of BGPmon does a good job of alerting for BGP hijacks[1] or router misconfigurations for a limited number (up to five) of prefixes, while the paid version of BGPmon has more capabilities but creates an additional cost burden for many small RLECs. BGPsec has even more capabilities. However, it is resource intensive and requires very expensive software that does not appear to be a justifiable investment by many RLECs particularly due to its lack of global support.

These latter WTA members are familiar with Resource Public Key Infrastructure ("RPKI") and Mutually Agreed Norms for Routing Security ("MANRS") recommended actions. Both of these measures can improve BGP security, but entail substantial complexities and time to implement while still leaving persistent BGP security gaps. Some members have adopted

[1] The Commission should distinguish between unlawful "BGP hijacking" for malicious purposes, and lawful BGP re-routing for maintenance and incident recovery purposes.

MANRS' recommended actions but are particularly reluctant to join MANRS because both its membership list and their specific security actions are publicly available.

Conclusion

WTA applauds the Commission for joining with other federal agencies to study the effectiveness and cost of various BGP improvements and alternatives to secure Internet traffic against malicious re-routing. It recommends that the Commission focus on providing advice and recommendations regarding available cybersecurity resources and up-to-date warnings regarding current cyberattack activities and tactics. WTA also believes that the Commission should require Tier 1 and Tier 2 networks to undertake predominant responsibility for BGP routing cybersecurity and thereby reduce vulnerabilities arising from the problem that many RLECs and other small service providers lack the staff and financial resources to maintain adequate defenses against increasingly sophisticated BGP routing cyberattacks. Finally, given the constantly changing nature of cyberattacks, the Commission should not adopt specific regulations and equipment requirements that can be rendered ineffective or useless by the time they are implemented.

Respectfully submitted,
WTA – ADVOCATES FOR RURAL BROADBAND

/s/ Derrick B. Owens
Senior Vice President of
Government and Industry Affairs
/s/ Eric Keber
Vice President of Government Affairs
400 Seventh Street NW, Suite 406
Washington, DC 20004
Phone: (202) 548-0202

/s/Gerard J. Duffy
Regulatory Counsel
Blooston, Mordkofsky, Dickens, Duffy &
Prendergast, LLP
2120 L Street NW, Suite 300
Washington, DC 20037
Phone: (202) 828-5528

Dated: April 11, 2022