Before the
Federal Communications Commission
Washington, D.C. 20554

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

COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Notice of Inquiry ("*Notice*")[2] released by the Federal Communications Commission ("Commission") in the above-captioned proceeding. The Commission issued the *Notice* to identify measures that can be taken to help secure Internet services against cyber threats. Specifically, the Commission sought comment on "vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP)" which, if misconfigured, could "allow a network operator to accidentally or maliciously misconfigure its BGP routers to falsely advertise that its network contains the intended destination for certain Internet traffic, or is on the path to that destination."[3]

NTCA supports the Commission's goal of helping to secure Internet traffic; however, NTCA encourages the Commission to carefully examine whether any proposed efforts to secure BGP would achieve the intended result and whether and to what degree any Commission

[1] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[2] *Secure Internet Routing,* Notice of Inquiry, PS Docket No. 22-90, FCC 22-18 (rel. Feb. 28, 2022).

[3] *Notice* at ¶ 5.

recommendations can be implemented across the service provider industry. To scope this effort properly, NTCA first encourages the Commission to clarify that "BGP hijacking" specifically requires malicious intent.[4] Without that, simply saying BGP hijacking exists when traffic is diverted from its most efficient path could inadvertently sweep in maintenance-type BGP rerouting, such as when traffic is diverted to a third-party data center for DoS traffic scrubbing, or configuration errors. Organizations and network operators need to retain the ability to perform periodic traffic engineering. Furthermore, any "hijacking" concerns arise not so much out of the routing of traffic between BGP speakers (which are typically directly adjacent over a mutually trusted path), but rather from a malicious third party that is able to advertise IP address space or traffic paths that it is not authorized to advertise.

The Commission referenced several efforts undertaken by Internet stakeholders to improve BGP security, including a recommendation by the Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC") that "network operators ensure that BGP routers' Internet routing registries are accurate, complete, and up-to-date, and that network operators use a standards-based approach for providing cryptographically secure registries of Internet resources and routing authorizations, a Resource Public Key Infrastructure (RPKI)."[5] There are two parts to implementing RPKI: (1) network operators signing their own IP ranges, and (2) only accepting prefixes that are signed. A network prefix "determines the number of IP addresses within a particular section of IP addresses."[6] Meanwhile, prefix filtering allows a

[4] *See Notice* at ¶ 5 ("Causing Internet traffic to depart from its most efficient path is termed 'BGP hijacking.'").

[5] *Notice* at ¶ 7.

[6] "What Are Network Prefixes," May 27, 2016, available at What are Network Prefixes?. What are network prefixes? | by Datapath.io | NetDevOps | Medium (last visited Apr. 6, 2022).

network administrator to permit or deny specific prefixes, thereby preventing IP traffic from being routed to unwanted or illegitimate routes.[7] Typically, modern routers support the signing of prefixes. Providers using routers with this capability should be able to implement RPKI fairly quickly. Network operators with older routers or routers that do not support the signing of prefixes, however, would likely need to invest in a newer router.[8]

Thus, the first part of RPKI implementation – signing IP ranges – may require some additional work and upgrading in certain cases but does not appear to present a significant barrier. Requiring smaller network operators to comply with the second part of RPKI, however, makes little sense as these operators' traffic typically routes through larger transit providers for distribution across the Internet. Furthermore, smaller operators typically do not provide BGP service to downstream customers. Instead, these operators could achieve a similar level of routing information protection by signing their routes to make those routes "RPKI valid" and acquiring service from Internet exchanges and providers that are filtering RPKI invalids. These techniques would provide smaller operators with much the same security without the need to purchase an RPKI-compatible server or have the technical expertise necessary to implement and update RPKI in their network. Thus, there would be little value in expecting small operators to re-verify what an Internet transit network has already verified nor would doing so improve security.

[7] A Guide to Border Gateway Protocol (BGP) Best Practices, National Security Agency Cybersecurity Report (Sep. 10, 2018), available at ctr-guide-to-border-gateway-protocol-best-practices.pdf (nsa.gov) (last visited Apr. 6, 2022), p. 11 ("NSA Cybersecurity Report").

[8] *See, e.g.*, Router Support – RPKI documentation, available at https://rpki.readthedocs.io/en/latest/ops/router-support.html (last visited Apr. 6, 2022).

The Commission also sought comment on the extent to which tools such as the National Institute of Standards and Technology's ("NIST's") RPKI Monitor, Automatic and Real-Time dEtection and Mitigation System ("ARTEMIS"), BGPstream, BGPMon, Kentik, and Traceroute are able to rapidly and accurately detect BGP hijacking or router misconfigurations and distinguish malicious routing changes from accidental ones.[9] While perhaps somewhat helpful, these tools can still leave gaps in security depending upon the number and diversity of data feeds they receive and the need to filter out alerts that reflect unique arrangements between operators. Additionally, they are generally unable to automatically identify malicious intrusion from a more straightforward error – meaning that the network operator must investigate further to determine whether and to what degree hijacking has occurred. [10]

The Commission further sought comment on why some network operators may not have taken more aggressive steps to implement BGP security measures such as RPKI and Mutually Agreed Norms for Routing Security ("MANRS"). There are several barriers worth noting, including the complication and time involved in implementing such measures and the fact that, even after doing so, BGP security gaps may persist. Moreover, not all routers support BGP security and RPKI requires a supporting/redundant server. Additionally, implementation of security measures can cause traffic outages for a portion of a provider's network while RPKI configuration issues are resolved and actual issues are uncovered. Furthermore, if a network's

[9] *Notice* at ¶ 9.

[10] *See, e.g.*, "Why Is it Taking So Long to Secure Internet Routing?," by Sharon Goldberg, Boston Univ. (Sep. 11. 2014), available at Why Is It Taking So Long to Secure Internet Routing? - ACM Queue (last visited April 1, 2022) ("the security benefits of BGPSEC apply only after *every* [network] on the path has deployed BGPSEC."); "BGP Security: the BGP sec Protocol," (Apr. 30, 2015), available at BGP security: the BGPsec protocol | Noction (last visited Apr. 1, 2022) ("Deployment of BGPsec will be challenging, as the protocol is quite resource-intensive. BGP updates will be larger due to the inclusion of signatures and supporting information.") "BGPSec and Reality," available at BGPsec and Reality – rule 11 reader (last visited Apr. 1, 2022).

prefix is accidentally filtered by another organization, traffic is affected. To feel comfortable implementing MANRS, network operators must be able to verify they have the ability to implement the actions advised by MANRS, which may require time, resources, and expertise that are not readily available. These all present operational and/or cost challenges to successful industry-wide implementation of BGP security measures.

The Commission also sought comment on the extent to which RPKI "effectively prevents hijacking."[11] Although RPKI uses cryptographic signatures to authenticate routing information, widespread deployment is necessary to achieve the most protection from this security measure. Analogous in some ways to the STIR/SHAKEN framework in terms of reliability of authentication, to be effective, BGP security measures require managing routes across all address registries, a difficult undertaking at best, combined with implementing multiple different solutions.[12] Indeed, the National Security Agency concluded in a 2018 report that:

> In order to mitigate the common threats …, most, if not all mitigations should be implemented. These mitigation methods include using access control lists … to only accept traffic from legitimate or known BGP neighbors, rate-limiting the flow of traffic to the router control plane to prevent the router resources from being overwhelmed by DoS attacks, validation and filtering of exchanged routing information, authentication amongst BGP neighbors to ensure the neighbors are authentic, and enabling logging to monitor BGP neighbor activities such as unauthorized changes in the event of an attack to the router.[13]

Finally, the Commission correctly suggests that coordinating with other federal agencies could help promote secure Internet routing.[14] For instance, the Commission and other federal

[11] *Notice* at ¶ 11.

[12] *See, e.g.*, "Microsoft Introduces Steps to Improve Internet Routing Security," Albert Greenberg, Dec. 9, 2020, available at https://azure.microsoft.com/en-us/blog/microsoft-introduces-steps-to-improve-internet-routing-security/ (last visited Apr. 6, 2022).

[13] NSA Cybersecurity Report at p. 6.

[14] *Notice* at ¶ 14.

agencies could offer workshops for both organizations that have BGP expertise and those that do not, offering guidance on how to implement secure routing practices. A number of smaller network operators have monitoring in place to detect BGP hijacking; however, implementing BGP security options such as RPKI or MANRS would require significant staff and financial resources. Similarly, even if those options could be outsourced reliably to a third party, the cost of doing so would likely be equally significant. Accordingly, educational workshops combined with subsidized training and implementation costs could help encourage implementation.

Based on the foregoing, NTCA recommends the Commission carefully consider what would be necessary from a technical and financial perspective for all network operators – especially small and medium-sized providers – to implement BGP security measures and whether and to what degree adoption of such security measures would achieve the intended result of securing all Internet traffic against malicious or unintended rerouting. Once the challenges are more thoroughly catalogued and the time and cost involved in overcoming them estimated, the Commission can begin to chart a path aimed at promoting the implementation of such measures.

Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Brian J. Ford
Tamber Ray

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203

(703) 351-2000