BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

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

COMMENTS OF INTERNET2

John S. Morabito
Danielle N. Rodier
Internet2
1150 18th Street, NW
Suite 750
Washington, DC 20036

Alan G. Fishel
Adam D. Bowser
ArentFox Schiff LLP
1717 K Street NW
Washington, DC 20006
Counsel for Internet2

Date: April 13, 2022

Internet2 submits these Comments in response to the Commission's Notice of Inquiry ("NOI") in the above-referenced docket.[1]

SUMMARY

Internet2 and the research and education ("R&E") networking community appreciate this opportunity to offer comments to assist the Commission in its efforts to protect the security of the nation's communication networks and critical infrastructure. As the Commission is aware, our community is a highly specialized sector with its own set of unique strengths and challenges. Therefore, Internet2 will highlight the current state of routing security in the R&E community and recommend several ways that the Commission can support the community as it attempts to improve upon the progress it has made already in this area.

The first and most important aspect of ensuring routing security is collaboration among network operators. A significant level of cooperation must exist between the hierarchy of network operators in the R&E community, from the last mile campus networks all the way to the national backbone level, to reduce the potential for a disruption in network services. However, the community would benefit from encouraging even more network operators to engage in these collaborative relationships.

R&E networks also face a unique set of legal and logistical barriers to implementing Border Gateway Protocol ("BGP") routing security measures. For example, since many of the R&E networks interconnected by Internet2 were some of the first and earliest adopters of internet technology, their IP numbers pre-date the American Registry for Internet Numbers ("ARIN"), and they do not have a current legal agreement to use its routing security features.

[1] *In the Matter of Secure Internet Routing*, PS Docket No. 22-90, Notice of Inquiry, FCC 22-18 (rel. Feb. 28, 2022) ("*NOI*").

Additionally, the over 1,000 independently managed networks interconnected by Internet2 are structured in a three-tier hierarchy of campus networks, state/regional middle mile R&E networks, and national R&E backbone networks (e.g., Internet2). Both the scale and structure of the R&E network community increase the need for coordination, awareness, expertise, and operational tools to achieve good routing security practices. While there have been significant improvements recently, Internet2 has come to understand that the R&E community should focus on improving two key metrics: the adoption of Resource Public Key Infrastructure Route Origin Authorizations ("RPKI ROAs") and the consistent registration of intended routing policy in Internet Routing Registries ("IRRs").

BACKGROUND ON INTERNET2

The University Corporation for Advanced Internet Development (d/b/a "Internet2") is a non-profit, member-driven advanced technology community, founded in 1996 by the nation's leading higher education institutions, that provides a secure high-speed network, cloud solutions, research support, and identity and access management services tailored for R&E. Internet2 helps U.S. R&E organizations solve shared technology challenges and develop innovative solutions in support of their educational, research, and community service missions. Internet2 also operates the nation's largest and fastest coast-to-coast national R&E network ("NREN"), which now serves 323 U.S. universities, 32 federal affiliates, and 46 regional and state education networks with speeds in increments of 400-800 gigabits per second. The network serves a critical niche in the national broadband infrastructure, underpinning high-capacity and advanced services for the demanding needs of research, education, and global collaboration.

In fact, of the more than 75,000 BGP-interconnected networks that make up the public internet, Internet2 ranks 54th globally for interconnecting networks and hosts.[2] A map of Internet2's current network, and the regional R&E networks that connect to it, can be found at: https://www.thequilt.net/wp-content/uploads/I2-Overlay-Quilt-Map-BW-web-11122018.pdf

Relevant to this proceeding, Internet2 operates the InCommon Federation, which facilitates secure, unified, and seamless single sign-on access to local, national, and global research and academic collaboration resources for more than 10 million users and more than 1,000 educational institutions, research organizations, and commercial resource providers in the U.S. InCommon makes possible trustworthy academic collaboration that reaches far beyond what a single organization can do on its own, through identity and access management technologies and services that are integrated across the globe. In addition, Internet2 is the operator of the eduroam service in the U.S., supporting millions of students, faculty, and staff with seamless roaming Wi-Fi at more than 1,000 colleges, universities, K-12 schools, museums, libraries, and research facilities across the country.

Further, Internet2 plays a key role as a convener and facilitator of the R&E community. Internet2 regularly brings together representatives from academia, federal agencies, and private industry to foster collaboration and find solutions to shared challenges related to R&E cyberinfrastructure that no single institution or organization could accomplish independently. In fact, Internet2 collaborates with a multitude of NREN partners that represent more than 100 countries across the globe.

Finally, Internet2 supports the R&E community through the Internet2 NET+ Cloud Services Program, which enables R&E institutions in adopting cloud solutions through a

[2] *See* https://asrank.caida.org.

streamlined process that minimizes the business, legal, financial, security, privacy, accessibility, and other challenges associated with migrating from on-campus to cloud-based solutions.

DISCUSSION

I. Routing Security Requires Collaboration

In Internet2's experience, the essential component of routing security is collaboration along the hierarchy of network operators. In the R&E networking context, university networks need to publish the routing policies of the resources they hold (e.g., IP Networks). Typically, these policies are published via IRRs and Regional Internet Registries (e.g., ARIN) as RPKI ROAs.

In general, the university network is linked to the state or regional network that provides the middle mile, connecting the university to the national backbone. These regional networks need to use the policies published by the universities to filter or enforce those policies at the regional level. The regional networks also need to aggregate and publish their members' routing policies.

These state or regional networks then connect to national networks. The national networks (e.g., Internet2) need to use the aggregated regional network policies, as well as their global view of policies published via RPKI ROAs, to establish filters that both prevent misconfigurations at the university or state network level from propagating and avert more global errors from impacting the state and university networks.

The goal of this collaborative relationship is to reduce the possibility of the disruption of network services due to a misconfiguration or intentional routing hijack by using RPKI. However, more coordination would be helpful in this area. For example, while Internet2 can implement the backbone side of RPKI by employing systems to monitor and drop routes that fail RPKI validation, this is only beneficial if individual networks create RPKI ROAs against which the RPKI validation operates. Today, only five percent of Internet2 service routes have RPKI ROAs.

II. Barriers to Deploying BGP Security Measures Unique to U.S. R&E Networks

The Commission seeks comment on obstacles to increasing BGP security.[3] In its experience facilitating greater collaboration on security issues facing the R&E community, Internet2 has identified the following barriers that have slowed the deployment of BGP security measures.

A. RPKI Legal Barriers

The R&E community collectively represents some of the first adopters of internet technology. Many of the over 1,000 networks interconnected by Internet2 were built in the 1980s, and they were assigned IP network numbers before ARIN was formed. These initial IP number authorizations are known as "legacy resources." ARIN permits these legacy resource holders to continue to use their IP network numbers without a formal agreement with ARIN. ARIN continues to allow these networks to maintain their basic "whois" information; however, without a current agreement covering these legacy resources, organizations cannot legally use ARIN's routing security features, such as RPKI and Authenticated IRR.

In fact, as documented by Christopher S. Yoo and David A. Wishnick in their publication "Lowering Legal Barriers to RPKI Adoption," legal barriers, including for example contractual provisions relating to indemnification, prevent or add significant friction to bringing legacy resources under an ARIN agreement.[4]

[3] NOI ¶ 12.

[4] *See* https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3037&context=faculty_scholarship.

B. Logistical Challenges

As previously noted, the R&E community is a large hierarchical collaboration of independently operated networks, which increasingly stands in contrast to monolithic residential and/or commercial ISPs of similar interconnectedness. Therefore, the R&E network community requires a higher degree of coordination to collectively achieve widescale adoption of routing security best practices.

III. Recommendations to Improve the State of Routing Security in the R&E Community

Given the challenges facing R&E networks detailed above, Internet2 has devoted significant resources to monitor and help improve security practices across the R&E networking ecosystem over the last several years. As part of these efforts, Internet2 regularly measures the adoption of routing security practices in the R&E community. There have been significant improvements over the last two years: the percentage of Internet2 regional networks that publish their routing policy has doubled and the quality (accuracy and consistency) of the published routing policies has improved by a factor of five. Nonetheless, the overall R&E community lags in two key metrics: the adoption of RPKI ROAs and the consistent registration of intended routing policy in IRRs.

By one measure, the percentage of routes with corresponding RPKI ROAs, the R&E network has one-fifth of internet adoption. Another measure of the community's adoption of routing security is the number of IP routes leaked (routes announced to Internet2 that represent misconfigurations or route hijack attempts) that Internet2 helps mitigate. These measurements depict an overall routing security posture that leaves room for improvement.

Further, in 2019, several networks, including Google, Hurricane Electric, and others, announced that their peers, like Internet2, must publish their routing policies via IRR or RPKI

ROAs to continue to use these connections. This required Internet2 to work with its regional/state networks to ensure that all of their members (e.g., universities, schools, hospitals, etc.) also published their routing policies. In response to this requirement, Internet2 developed a route report to identify how regional/state networks and their members were meeting these requirements. Internet2 uses these reports to inform its outreach to regional/state networks and their members to assist with their ability to publish their routing policies and improve overall security practices. However, even with these improvements, the adoption of routing security remains low. Based on its experience, Internet2 recommends that the FCC support the following five-point plan for improving R&E routing security through a sustained community-driven effort that would result in:

1. *Making the concepts of routing security accessible and important.* Routing security does not appear in the context of HIPAA, PCI DSS, FERPA, CSA or other industry or regulatory compliance frameworks or specifications. Hence, many organizations are unaware of routing security and the collaborative role they play in ensuring the reliable operation of the internet. While the National Institute of Standards and Technology, MANRS.org, and others have created helpful resources to inform routing security practice, the topic has not achieved the same level of awareness as compared to other cybersecurity threats.[5] The Commission, and related arms of the federal government, can play a role in helping to educate the R&E community that good routing security is critical to its network-centric infrastructure.

2. *Access to router configuration training.* Specifically, training is necessary to configure and operate multi-homed BGP networks that implement best practices to ensure

[5] *See* https://www.nccoe.nist.gov/publication/1800-14/VolB/index.html, "Protecting the Integrity of Internet Routing."

correct routing policy and community practices to synchronize traffic engineering.

3. *The development and adoption of network configuration tools that will aid in the consistent implementation of the desired routing policy.* Without accessible network automation tools, at best networks will obtain an acceptable degree of routing security at a point in time, then drift into states of lesser and lesser security as the inputs (e.g., IRR records, bogon lists, records of customer IP networks, etc.) change over time. More commonly, without automation, networks will achieve inconsistent and low degrees of routing security.

4. *The development and operation of an R&E routing security observatory to provide the ability to independently measure the alignment with secure route policy.* The R&E community's approach to operation transparency is far more permissive than the commercial sector. For example, while commercial backbone providers host "looking glass" servers, allowing users to inspect the routing state of their network, Internet2 hosts a "router proxy" that allows users to fully inspect all of the routing and performance parameters of individual backbone routers. An R&E routing security observatory would expand upon MANRS Observatory's features to include routing information unique to R&E networks (generally greater use of more specific announcements used to affect traffic engineering), as well as offer a deeper look into the routing and security state of the entire R&E network community.

5. *The development and maintenance of an R&E routing security control framework for assessing an organization's routing security.* While security control frameworks exist for different service model paradigms (e.g., the Cloud Security Alliance Cloud Controls Matrix), a similar framework does not exist for assessing the routing integrity and security of an organization's network.

CONCLUSION

For 25 years, the R&E community has worked together in a highly collaborative manner to meet the networking needs of research and education. Internet2, as a trusted partner in this community, shares its insights and knowledge and coordinates the development of advanced services with 1,000 interconnected networks openly and transparently. The approach for improving the R&E community's routing security should leverage these traits. Internet2 is optimistic that with the leadership of the Commission these barriers can be addressed successfully. Internet2 looks forward to working with the Commission on this important matter.

Respectfully submitted,

/s/ John S. Morabito
John S. Morabito
Vice President and General Counsel
Internet2
1150 18th Street, NW
Suite 750
Washington, DC 20036