Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Reporting on Border Gateway Protocol Risk	)	PS Docket No. 24-146
Mitigation Project	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90

Comments of the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Stephanie Weiner
Chief Counsel

Alan Davidson
Assistant Secretary of Commerce
for Communications and Information

Travis Hall, Acting Associate Administrator
Office of Policy Analysis and Development

Robert Cannon
Telecommunications Policy Analyst
Office of Policy Analysis and Development

National Telecommunications
and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230
202.482.1816

July 17, 2024

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Reporting on Border Gateway Protocol Risk Mitigation Project	)	PS Docket No. 24-146
	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90

Comments of the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

I. SUMMARY

The National Telecommunications and Information Administration (NTIA) is pleased to offer the Administration’s comments in response to the Notice of Proposed Rulemaking (NPRM) in the above-captioned proceeding.[1]

The United States Government is tackling the “pervasive concern” of routing security. We are realizing the benefits of decades of U.S. Government investment and collaboration with stakeholders. U.S. network operators are making progress, but there is more work to be done. Misaligned incentives have led to low rates of Route Origin Authorization (ROA) adoption by certain large network operators. The Administration supports properly implemented and narrowly constructed Border Gateway Protocol (BGP) reporting requirements created by the Federal Communications Commission (FCC) as a means of addressing low ROA adoption by select large Broadband Internet Access Service (BIAS) providers. The FCC’s action should be appropriately tailored to preserve the highly successful multistakeholder model of Internet

[1] *Reporting on Border Gateway Protocol Risk Mitigation Progress*, PS Docket No. 24-136, Notice of Proposed Rulemaking (2024) (*Reporting on BGP NPRM*).

governance and should be consistent with the three principles that NTIA laid out in its Open Internet comments.[2]

II. MATURE ROUTING SECURITY SOLUTIONS CAN MITIGATE THE RISK OF ROUTING VULNERABILITIES

Networks create a map of the Internet by sharing route information using BGP. Networks announce to each other that a *destination* is found on that network or that they are *a route to another network* where a destination is found. Both the information about the *destination* and the *route* to the destination can be false. Over 100,000 Internet networks share routing information, creating a complex map of the Internet. Most routing incidents are accidental; some are malicious.[3]

A BGP origin announcement is an announcement by a network that a destination is found on that network (it pairs an Internet address block or prefix (the destination) – with an autonomous system number (ASN) (the network)). For example, NTIA (prefix 198.51.11.0/24) is a destination found on the National Oceanic and Atmospheric Administration (NOAA) N-Wave network (ASN 3477). However, any other network anywhere could also make a BGP

[2] We urged the Commission to (1) ensure it is collaborating closely with relevant Executive Branch agencies; (2) continue to rely primarily on partnerships with the private sector, particularly via longstanding multistakeholder processes; and (3) develop narrowly-tailored regulatory solutions when voluntary initiatives fail and other agencies cannot address the problem. *See* Ex Parte Comments of NTIA, *Safeguarding and Securing the Open Internet*, WC Docket 23-320, at 7 (filed March 20, 2024), https://www.ntia.gov/sites/default/files/publications/ntia_title_ii_comment.pdf (*NTIA OI Comments*).

[3] The oft cited Pakistan Telecom / YouTube 2008 incident was an attempt at domestic censorship that was accidentally leaked to the international Internet. According to the BITAG Report, "Perhaps the most famous BGP route-hijack occurred in February 2008, involving the state telecom of Pakistan (PTCL) and YouTube. In that instance, the government of Pakistan ordered that access to YouTube be blocked within the country because of a video it insisted on preventing its citizens from accessing. To implement the block, PTCL announced more-specific prefixes for YouTube's BGP routes in order to divert Pakistan's domestic traffic bound for the video streaming service to an alternate destination within their own network. Once hijacked, PTCL's goal was to drop Pakistani YouTube users' packets, preventing them from accessing YouTube. What was planned as an intentional route-hijack through prefix-manipulation inside Pakistan took on global ramifications when PCTL accidentally leaked these routes to its international transit providers, who carried the routes around the world and thereby blocked YouTube for a large portion of the global Internet." *"Security of the Internet's Routing Infrastructure,"* Broadband Internet Technical Advisory Group, p. 13 (2022), https://www.bitag.org/Routing_Security.php (*BITAG Report*).

announcement that NTIA is a destination on their network. Nothing about BGP authenticates which announcement is valid.

The Regional Internet Registries (RIRs) manage Internet number resources (i.e., IPv4 addresses, IPv6 addresses, and autonomous system numbers). As the authoritative directories of address resources, the RIRs offer the routing security solution Resource Public Key Infrastructure (RPKI): Route Origin Authorization (ROA). A ROA is a cryptographically verifiable statement, created by the holder of an Internet address block, that a destination (a prefix) is found on a specific network. For example, NTIA created a ROA that NTIA is a destination on the NOAA N-Wave network.

This leads to two sets of data: (1) BGP announcements which are not validated, and (2) cryptographically verifiable ROAs. Upstream networks which receive BGP origin announcements can compare them against ROAs in a process known as Route Origin Validation (ROV). If the BGP announcement agrees with the ROA, it is valid (the upstream network will add itself to the route path and propagate the announcement to its neighbor networks that it is a route to the network where the destination can be found. In other words, it will announce, "you can get there through me."). If the announcement is invalid, it is filtered. If, for example, any other network falsely announces that NTIA is a destination on its network, an upstream network's ROV process will produce an invalid result; the false announcement will get ignored.

ROAs are one solution that effectively addresses one set of vulnerabilities: accidental misconfigurations of origin announcements.[4] ROAs do not, for example, validate route paths or

[4] *See* Philip Gervasi, *Breaking the 50% Barrier: an RPKI ROV Discussion with Job Snijders and Doug Madory*, Telemetry Now, Season 2, Episode 6 (June 20, 2024), https://www.kentik.com/telemetrynow/s02-e06/ (Doug Madory stating that RPKI ROV limits accidental originations such as inadvertent fat finger mistakes. Routing security experts should be very careful to not overstate what RPKI ROV will do for routing. Routing security experts don't want to oversell RPKI ROV as a silver bullet. A determined adversary can defeat it.).

stop route leaks. There is no silver bullet. RPKI should be a part of a larger routing security strategy, and routing security should be part of a network operator's larger network security and reliability strategy.[5]

The Mutually Agreed Norms of Routing Security (MANRS), a project of the Internet Society and the Global Cyber Alliance, sets forth four mature baseline actions that any network can effectively and affordably implement.[6] These recommended actions include ROAs, updating contact information in routing databases, ensuring that customers only announce Internet addresses they are authorized to announce, and preventing traffic with spoofed IP addresses. ROAs have been described as a few minutes' worth of work to avoid millions of dollars' worth of harm.

ROV filtering creates positive externalities. Consequently, not every network needs to do ROV.[7] Core transit networks, generally Tier 1 transit networks and larger Tier 2 transit networks, provide access to the full routing table and carry lots of traffic. They receive lots of routing announcements, add themselves to the route path, and then propagate those announcements further to interconnected network partners. When core networks implement routing security, it has strong positive externalities, benefiting everyone that would use those transit providers as a path to a destination. It benefits everyone downstream: their customers and the customers of their customers. Because core networks have deployed ROV filters and other

[5] *See* National Institute of Standards & Technology, NIST CSWP 29, *The NIST Cybersecurity Framework (CSF) 2.0* (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[6] *Network Operator Actions*, MANRS, https://manrs.org/netops/network-operator-actions/.

[7] *See, e.g.*, Job Snijders, *Routing Security Roadmap* , LACNIC 30 (2018), https://www.lacnic.net/innovaportal/file/3135/1/lacnic30_snijders_routing_security_roadmap.pdf ("Not everyone needs to do RPKI [ROV]; Because of the centralization of the web, if a select few companies deploy RPKI Origin Validation – millions of people benefit.").

solutions, we have observed improvements in routing security.[8] Conversely, there is essentially no positive externality benefit for stub networks (networks that do not provide transit service to any downstream customer networks) deploying ROV filtering. Thus, there is a spectrum of positive externality benefits to ROV, with filtering by the top core networks resulting in the greatest benefit and diminishing benefits as networks are positioned closer to the edge of the Internet.

III. THE U.S. GOVERNMENT IS REALIZING THE BENEFITS OF DECADES OF INVESTMENT AND COLLABORATION WITH STAKEHOLDERS

In 2003, the White House stated that BGP "is at greatest risk of being the target of attacks designed to disrupt or degrade service on a large scale."[9] In response, the National Institute of Standards and Technology (NIST) and the Department of Homeland Security's Science and Technology Directorate funded and collaborated with stakeholders, developing technical solutions and guidance.[10] The FCC worked with stakeholders through its federal advisory committee, the Communications Security Reliability and Interoperability Council (CSRIC), to develop best practices.[11] The National Science Foundation funded academic routing security research.

[8] *See, e.g.*, Doug Madory*, Exploring the Latest RPKI:ROV Adoption Numbers 2023,* Kentik Blog (May 24, 2023), https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/ ("Due to the immense scale of these backbone providers, they end up shielding much of the Internet from RPKI-invalid routes.").

[9] The Executive Office of the President, *The National Strategy to Secure Cyberspace* at 30 (2003), https://georgewbush-whitehouse.archives.gov/pcipb/.

[10] *See* DHS Science & Technology Directorate, *Secure Protocols for Routing Security Infrastructure* (accessed June 20, 2024), https://www.dhs.gov/publication/secure-protocols-routing-infrastructure; NIST, *Robust Internet-Domain Routing* (accessed June 20, 2024), https://www.nist.gov/programs-projects/robust-inter-domain-routing.

[11] *See Reporting on BGP NPRM,* para 20, *et. seq*.

We are realizing the benefits of decades of U.S. Government investment and collaboration with stakeholders.[12] However, there is more work to be done. The 2023 National Cybersecurity Strategy referred to routing security as a "pervasive concern" and that routing security requires

> close collaboration between public and private sectors to reduce our risk exposure without disrupting the platforms and services built atop this infrastructure. The Federal Government will lead by ensuring that its networks have implemented these and other security measures while partnering with stakeholders to develop and drive adoption of solutions that will improve the security of the Internet ecosystem and support research to understand and address reasons for slow adoption.[13]

National Cybersecurity Strategy Initiative 4.1.5 called on the Office of the National Cyber Director (ONCD), "in conjunction with key stakeholders and appropriate Federal Government entities, [to] develop a roadmap to increase the adoption of secure Internet routing techniques and technology."[14]

We are making progress towards improved routing security.[15] The Internet community has engaged in robust outreach to promote greater security.[16] The percentage of global

[12] *NTIA OI Comments* at 4 ("The lightning-fast evolution of our communications technologies and our growing dependence on these offerings necessitate a whole-of-government approach to security that engages all available federal government resources.").

[13] Executive Office of the President, *National Cybersecurity Strategy,* at 22-23 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (*National Cybersecurity Strategy*).

[14] Executive Office of the President, *National Cybersecurity Strategy Implementation Plan*, at 38 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

[15] *See Reporting on BGP NPRM*, para. 35.

[16] For example, in 2023, the North American Network Operators Group (NANOG) had approximately 15 sessions on routing security at its three conferences; it had more presentations on routing security than any other subject. *Past NANOG Events*, NANOG (accessed June 21, 2024), https://nanog.org/events/past/. The MANRS Community Report 2023 reports that MANRS has grown to 1073 participants, adding 195 participants in 2023. MANRS reports that "in 2023, the MANRS team and MANRS mentors and ambassadors presented at nearly 50 in-person and virtual events across six continents and held a record five MANRS community meetings, including the first community-led meeting in the Latin America region." MANRS, *Community Report 2023*, at 3, 8 (2024), https://manrs.org/wp-content/uploads/2024/01/MANRS-Community-Report_2023.pdf.

destinations protected by ROAs is now over 51%.[17] The percentage of Internet global traffic covered by ROAs has, according to Kentik, grown to 70.3%.[18] The number of networks enabling RPKI service on their American Registry for Internet Numbers (ARIN) accounts is up.[19] In North America, the percentage of destinations protected by ROAs is 39% for IPv4 and 53% for IPv6.[20] North America has approximately 113,000 ROAs; more than twice as many as the next largest region, RIPE (Europe), with approximately 45,000 ROAs.[21] All Tier 1 networks and a significant number of Tier 2 networks based in the United States have deployed ROV filtering.[22] False destination announcements have had an increasingly hard time spreading through the network.[23] Finally, with 39% ROAs and 100% ROV by USA-based Tier 1 transit providers, according to the MANRS Observatory, over the last two years routing incidents have been trending down.[24]

[17] *NIST RPKI Monitor*, NIST, (accessed June 21, 2024), https://rpki-monitor.antd.nist.gov/.

[18] Doug Madory, Job Snijders, *RPKI ROV Deployment Reaches Major Milestone*, Kentik Blog (May 1, 2024), https://www.kentik.com/blog/rpki-rov-deployment-reaches-major-milestone/ (up from 56% of traffic RPKI valid two years ago).

[19] John Sweeting, *ARIN Update*, NANOG 91, Slide 28 (June 10, 2024), https://storage.googleapis.com/site-media-prod/meetings/NANOG91/5109/20240608_Sweeting_Arin_Update_v1.pdf (In 2022 there were 891 new RPKI registrations; in 2023 there were 1453 new registrations. As of May 31, 2024, there were already 724 new registrations. As of Q1 2024, total RPKI registrations had reached 4879) (*ARIN Update*).

[20] NIST, *NIST RPKI Monitor*, https://rpki-monitor.antd.nist.gov/ROV/20240521.00/A/All/4 (data as of June 21, 2024) *See also* MANRS Observatory, https://observatory.manrs.org/#/overview (accessed June 21, 2024) (38% of USA prefixes protected by RPKI).

[21] NLNet Labs, *Routinator: Metrics* (accessed June 21, 2024), https://rpki-validator.ripe.net/ui/metrics.

[22] According to RoVista, all Tier 1 networks, except for Telecom Italia Sparkle, receive ROV scores of 100%. RoVista, (accessed June 21, 2024) https://rovista.netsecurelab.org/. *See also* RoVista Analytics, Rovista (accessed June 21, 2024), https://rovista.netsecurelab.org/analytics (United States: 91.58 ROV Score weighted average based on Cone Size of ASes; 67.9 weighted average of ROV score based on Internet addresses of ASes).

[23] Madory, *supra* note 18.

[24] *MANRS Observatory History* (accessed June 11, 2024), https://observatory.manrs.org/#/history (MANRS Observatory two year data for the United States shows 323 routing incidents in March 2022 trending down to 186 incidents in March 2024, with the elimination of large spikes of routing incidents).

Internet routing and routing security are complex. As recognized by the National Cybersecurity Strategy, success has been realized through "close collaboration between public and private sectors." Working with the expertise of network engineers and operators, the U.S. Government has been able to achieve mature solutions to routing security. As recognized by the *Declaration for the Future of the Internet*, a high level of security of the technical infrastructure of the Internet is only achieved by working closely with the multistakeholder system of Internet governance.[25] The FCC should, as previously recommended by NTIA, "continue to oversee a broad and inclusive approach to national security matters, recognizing the expertise and information possessed by private-sector experts and governmental partners both within and beyond the Executive Branch."[26] U.S. Government leadership on Internet policy establishes an example that will be followed internationally.

A. COMPETING PRIORITIES AND MISALIGNED INCENTIVES HAVE RESULTED IN LOW ROA ADOPTION RATES ON CERTAIN LARGE NETWORKS

More work needs to be done, as certain large network operators have poor ROA adoption rates. The U.S. Government has secured a small percentage of its destinations with ROAs.[27] Likewise, several large BIAS providers with complex Internet address inventories have low

[25] *See Declaration for the Future of the Internet,* U.S. Department of State (2022), https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf.

[26] *NTIA OI Comments* at 6.

[27] *See Reporting on BGP NPRM*, para. 35; Jen Easterly, Jessica Rosenworcel, *The Most Important Part of the Internet You've Probably Never Heard Of* (2023), https://www.cisa.gov/news-events/news/most-important-part-internet-youve-probably-never-heard ("we fully acknowledge that the U.S. government is lagging behind on BGP security practices").

levels of ROA adoption. Feedback from network operators is that competing priorities, misaligned incentives and barriers to adoption have led to stuck ROA adoption.[28]

The following is a *sample* of data of the nine identified providers.[29] The nine identified providers make up approximately 90% of the BIAS subscriber market; the remaining 2,200 BIAS providers[30] make up the rest of the market. The table below identifies large BIAS providers with insufficient ROA adoption.[31]

The most significant way for the FCC to further significantly reduce routing incidents is to address the misaligned incentives of those large providers.[32] The most significant way for the U.S. government to significantly reduce routing incidents is to implement routing security on federal networks and to require routing security from federal vendors. As noted above, the

[28] *See, e.g.*, MANRS, *Draft 1 – Routing Resilience Manifesto* (2014), https://manrs.org/about/draft1/ ("Security in general is a difficult area when it comes to incentives. Security of the global Internet infrastructure, be it DNS or routing, brings additional challenges: the utility of security measures depends on coordinated actions of many other parties.").

[29] Each provider has many AS networks – this is a sample of a large AS network for each provider. Results are dependent upon methodology. A provider's total progress will be the aggregation of all networks. Data was observed June 21, 2024. Each ASN is a mixture of addresses held by the provider and held by customers. "N/F" means the provider was not found as a participant of MANRS. MANRS scores are across all AS networks of the MANRS participant. "T1" notes that the referenced network is a Tier 1 provider. ASN links are to NIST. Sources: MANRS*, Network Operator Participants* (accessed June 21, 2024)*, https://manrs.org/netops/participants/;* Hurricane Electric (HE), *Hurricane Electric BGP Toolkit* (accessed June 21, 2024), https://bgp.he.net/; RoVista, *AS-Specific ROV Filtering Ratio* (accessed June 21, 2024), https://rovista.netsecurelab.org/AS/ ("RoV Scores are determined based on the number of RPKI-invalid prefixes reachable by an Autonomous System (AS). Consequently, a higher ROV score suggests that the AS can effectively filter more RPKI-IP prefixes. However, it is important to note that the RoV score does not conclusively indicate whether an AS has actually implemented ROV or not…").

[30] *Reporting on BGP NPRM*, para. 89.

[31] *See also* Doug Madory, *Dissecting the FCC's Proposal to Improve BGP Security*, Kentik Blog (July 10, 2024), https://www.kentik.com/blog/dissecting-the-fccs-proposal-to-improve-bgp-security/ (presenting an analysis of the nine BIAS providers in terms of BGP routes and traffic statistics).

[32] The good routing security of these large BIAS providers would impact the ecosystem and creates incentives for their networking partners to implement good security. For example, the U.S. Government received presentations from many content providers who contractually required their partners to implement routing security. *See, e.g.*, FCC, *FCC & CISA Border Gateway Protocol Security Workshop* (July 31, 2023), https://www.fcc.gov/news-events/events/2023/07/bgp-security-workshop.

current 39% ROA adoption rate has proven effective at decreasing routing incidents. The efforts of the U.S. Government and the FCC together, correcting the problem of large networks with low rates of ROAs, will greatly advance the policy objectives of further decreased routing incidents.

Network	ASN	MANRS#1 Filtering	MANRS#2 Spoofing	MANRS#3 Coordination	MANRS# 4 RPKI	Valid Prefixes (HE)	ROV Score (RoVista)
AT&T, Inc. [T1]	7018	N/F	N/F	N/F	N/F	31%	100%
Altice USA (Cablevision)	6128	N/F	N/F	N/F	N/F	72%	0%
Charter	7843	🟩	100%	100%	90%	88%	100%
Comcast	7015	🟩	100%	100%	94%	96%	100%
Cox	22773	N/F	N/F	N/F	N/F	97%	0%
Lumen [T1]	3356	🟩	100%	100%	3%	8%	100%
T-Mobile USA	21928	N/F	N/F	N/F	N/F	99%	67%
Telephone & Data Systems (including US Cellular)	4181	🟩	100%	100%	100%	99%	100%
Verizon [T1]	701	🟩	100%	100%	78%	78%	100%

The objective of U.S. Government policy, including FCC policy, is to reduce routing incidents. The adoption of mature routing security solutions is a means of getting there. The FCC's approach is designed to promote routing security by making routing security a priority and re-aligning incentives. The FCC should clearly set forth objectives of its routing security policy.

B. THE U.S. GOVERNMENT IS IMPROVING ROUTING SECURITY ON FEDERAL NETWORKS TO REDUCE ROUTING INCIDENTS

The U.S. Government is working to improve routing security on federal networks. Federal implementation of routing security can help secure federal networks, promote routing security, drive demand, reduce average costs, and establish de facto standards.[33] The General Services Administration created a template contract for acquiring routing security services from ARIN.[34] ONCD has engaged in outreach to federal agencies and will be setting forth a policy that calls on all federal networks to implement routing security.[35] The Department of Commerce has been leading federal efforts: NIST continues to engage the Internet engineering community to advance routing security solutions.[36] NOAA N-Wave, the first federal network to robustly implement routing security,[37] produced a playbook providing guidance for federal agencies on implementation.[38] NOAA updated the Department of Commerce Chief Information Officers Council on routing security and held a routing security panel at its recent N-Wave conference.[39]

[33] *See, e.g.*, Internet Society, *Input on U.S. Government's Routing Security Roadmap* (Dec. 2023) ("The U.S. Government can greatly incentivize the private sector to implement best practices by making routing security best practices a procurement requirement for network services.").

[34] *See Registration Services Agreement (RSA) FAQs,* ARIN (accessed June 7, 2024), https://www.arin.net/about/corporate/agreements/rsa_faq/ ("ARIN accommodates the unique circumstance of federal, state, or provincial governmental entities, and has a practice of modifying RSAs for such requirements.").

[35] *Reporting on BGP NPRM*, para. 29. NSF also encourages grantees to implement the MANRS Actions. *See* National Science Foundation, *NSF 24-530: Campus Cyberinfrastructure (CC*) Program Solicitation* (2024), https://new.nsf.gov/funding/opportunities/campus-cyberinfrastructure-cc/nsf24-530/solicitation. The Networking and Information Technology Research and Development (NITRD) federal advisory committee Joint Engineering Team (JET) has also been promoting routing security to its research and engineering community. *See* NITRD, *Joint Engineering Team (JET) Meetings 2023* (last visited July 5, 2024), https://www.nitrd.gov/coordination-areas/lsn/jet/jet-meetings-2023/ (listing presentations by MANRS and Internet2).

[36] *See* NIST, *Robust Internet Domain Routing: Associated Products* (accessed June 7, 2024), https://www.nist.gov/programs-projects/robust-inter-domain-routing/associated-products.

[37] *See Security Updates & New Initiatives,* N-Wave News, p. 6 (Nov. 2022), https://www.noaa.gov/sites/default/files/2023-09/N-Wave-Nov-Newsletter-2022.pdf.

[38] NOAA N-Wave, *Federal Resource Public Key Infrastructure (RPKI) Playbook*, Ver. 1.3 (May 2024), https://www.noaa.gov/sites/default/files/2024-06/FINAL-Federal-RPKI-Playbook-May-2024.pdf.

[39] NOAA N-Wave, *"Resource Public Key Infrastructure (RPKI) Playbook"* (Stakeholders & Science Engagement Summit, May 14-16, 2024), https://www.noaa.gov/organization/information-technology/n-wave-stakeholders-and-science-engagement-summit/2024-stakeholders-science-engagement-summit-meeting-agenda.

The Department of Commerce hosted a "Route Signing Day" in order to celebrate the renewed effort, pursuant to the National Strategy, of federal agencies implementing routing security.[40]

C. IMPLEMENTATION OF A NARROW AND APPROPRIATELY TARGETED FCC REPORTING REQUIREMENT CAN IMPROVE BIAS PROVIDER SECURITY AND PREVENT ROUTING INCIDENTS

The FCC should set forth what the objectives of its initiative are in order to properly determine whether the requirements are reasonably and narrowly tailored to achieve the goals of that policy. As NTIA stated in its Open Internet *ex parte*,

> To the extent that regulations are necessary, they should be narrowly tailored to the particular problem that must be addressed and should take into consideration the significant relevant policies, programs, and authorities that exist across Executive Branch agencies, as well as the highly successful and effective collaborations between the private sector and government agencies.[41]

Clearly articulated policy objectives are also necessary to identify when the success of the program has been achieved.

Implementation of a narrow and appropriately targeted FCC reporting requirement can effectively address misaligned incentives of large BIAS providers with low ROA adoption. The proposed reporting requirement responds to the problem of stuck ROA creation by raising awareness, prioritizing the creation of ROAs, and responding to misaligned incentives.

A light touch approach to this problem would align with long-standing U.S. Government policy in support of the multistakeholder approach to Internet governance. It should not mandate specific actions but leave it to network operators to develop strategies. Reporting requirements are an effective solution that the FCC has employed before to respond to reliability concerns.[42]

[40] Press Release, NTIA, *U.S. Department of Commerce Implements Internet Routing Security* (May 13, 2024), https://www.ntia.gov/press-release/2024/us-department-commerce-implements-internet-routing-security.

[41] *NTIA OI Comments* at 6-7.

[42] *See, e.g.*, *Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, Report and Order, Docket 13-75, 28 FCC Rcd 17476 (2013).

There are other potential routing security solutions on the horizon.[43] The FCC reporting requirement should focus on mature solutions that are achievable today (speculating on future solutions would not be a useful part of a BIAS provider's plan for deploying existing routing security solutions).

Government action, including FCC rules, should place network operators in the best position to nimbly defend against future vulnerabilities or attacks. Network operators are in the best position to determine effective security strategies for their networks and take actions based on evolving threats. Any FCC reporting requirement should afford network operators the agility to devise their own security strategies to effectively address vulnerabilities.

When the objectives of the FCC's policy are achieved, the requirements should sunset.[44] Continuing requirements would not benefit routing security while sunsetting these provisions would enable providers to dedicate resources to other objectives and permit the agility to respond to evolving technological challenges.

D. THE FCC SHOULD FACILITATE ROUTING SECURITY BY LOWERING BARRIERS TO ADOPTION

The FCC can further facilitate adoption of routing security by lowering barriers to adoption. Small networks have limited resources and staff.[45] Minimizing costs and administrative efforts can facilitate adoption while maximizing the resources small networks

[43] *See, e.g.*, Organisation for Economic Cooperation and Development (OECD), Routing Security: BGP Incidents, Mitigation Techniques and Policy Actions at 29-30 (2022), https://www.oecd-ilibrary.org/docserver/40be69c8-en.pdf ("BGPsec is not ready for widespread deployment."); *BITAG Report* at 25 ("At the time of this report, ASPA has not been adopted as an IETF standard.").

[44] The FCC's Policy objectives are not advanced by having BIAS providers with high routing security implementation report on their routing security strategies; these BIAS providers are not suffering from misaligned incentives. The FCC can easily monitor the routing security of these providers through publicly available resources.

[45] *National Cybersecurity Strategy* at 4 ("Individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity").

have available to dedicate to expansion of broadband Internet service to all Americans and other security concerns. Routing security should not be a zero-sum game where gains in routing security come at the cost of other priorities.

We support the FCC reducing the costs of information by supporting outreach, training, guidance, best practices and monitoring.[46] The FCC should collaborate with existing stakeholder efforts and incorporate them into FCC outreach efforts.[47]

We support the FCC making the reporting requirement for smaller providers easier by creating a standardized template for BIAS providers' BGP plans.[48]

Most of the data which the FCC seeks is available from publicly accessible databases.[49] Data from publicly available databases can be preferrable over reported data; it can produce higher quality data than reported data, is real-time information, and can be acquired directly from authoritative sources. Entities including ARIN, Internet2, NIST and MANRS use this data to create scorecards for constituencies.[50] The FCC should rely on this data to analyze the progress of BIAS providers. The FCC should use this data to identify low performing BIAS providers and focus on addressing those providers' performance. Conversely, the FCC should use this data to identify BIAS providers with high levels of routing security that are not part of the problem and

[46] *Reporting on BGP NPRM*, para. 78, *et. seq*; Internet Society, *Routing Security for Policy Makers,* Internet Society White Paper at 6 (Oct. 24, 2018), https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/ ("Stakeholders should support the development of better mechanisms for information sharing, engage in information sharing on routing security, and collaborate with stakeholders to address routing security threats.").

[47] The FCC has previously collaborated with stakeholders on other successful outreach campaigns. *See, e.g.*, FCC, *Digital Television* (accessed July 5, 2024); FCC, *Y2K Communications Sector Report* (1999), https://transition.fcc.gov/nric/nric-4/y2k-communications-sector-report.pdf.

[48] *Reporting on BGP NPRM*, para. 41.

[49] *Reporting on BGP NPRM*, para. 46.

[50] *See, e.g.*, NIST, *RPKI Monitor 2.0, Methodology and User's Guide* (accessed June 10, 2024), https://rpki-monitor.antd.nist.gov/Methodology (describing sources for NIST's RPKI Monitor).

should not be encumbered with regulatory compliance obligations. It is unnecessary for the FCC to create a reporting requirement for data which is already publicly available.

The FCC should allow stakeholders to identify a safe harbor report. For example, a MANRS Observatory report card could potentially satisfy FCC requirements.

We support the FCC adopting a risk-based approach.[51] For example, not all prefixes are associated with the same amount of traffic, some prefixes are associated with critical infrastructure, and some networks' prefixes are subject to more change.[52] Any obligations should reflect the different risks of different Internet address blocks.

IV. CONCLUSION

Routing security is a pervasive concern for which there are mature technical solutions. U.S. network operators are making progress, but more work needs to be done. Misaligned incentives have led to low rates of ROA adoption by certain network operators. The Administration supports properly implemented and narrowly constructed BGP reporting requirements created by the FCC as a means of addressing low ROA adoption by select large BIAS providers while respecting long-standing support for the multistakeholder system of Internet governance.

All network providers should improve their routing security by creating ROAs for their Internet prefixes. The MANRS Actions for Network Operators are excellent baseline actions any network can affordably implement.

[51] *Reporting on BGP NPRM*, para. 38.

[52] Madory, *supra* note 18.

Respectfully Submitted,

Stephanie Weiner
Chief Counsel

Alan Davidson
Assistant Secretary of Commerce
for Communications and Information

Travis Hall, Acting Associate Administrator
Office of Policy Analysis and Development

Robert Cannon, Telecommunications Policy Analyst
Office of Policy Analysis and Development

National Telecommunications
and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230
202.482.1816

July 17, 2024