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

In the Matter of	
Matter of Safeguarding and Securing the Open Internet	WC Docket No. 23-320
Restoring Internet Freedom	WC Docket No. 17-108

EX PARTE COMMENTS OF THE INTERNET SOCIETY AND THE GLOBAL CYBER ALLIANCE

The Internet Society[1] and the Global Cyber Alliance[2] submit these comments to respond to and express serious concerns about the apparent intention of the Federal Communications Commission to consider imposing regulations concerning Internet routing security and the Border Gateway Protocol (BGP), as indicated in paragraph 46 of the Commission's draft Declaratory Ruling, Order, Report and Order, and Order on Reconsideration ("the Declaratory Ruling and Order"), in the Matters of Safeguarding and Securing the Open Internet Restoring Internet Freedom ("the Open Internet Proceeding").[3]

[1] Founded in 1992 by a number of the original architects of the Internet, the Internet Society is a global nonprofit organization dedicated to ensuring the open development, evolution, and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that protect the Internet. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

[2] The Global Cyber Alliance is a nonprofit organization dedicated to making the Internet a safer place by reducing cyber risk. We build programs, tools, and partnerships to sustain a trustworthy Internet to enable social and economic progress for all. Since January 2024, it has taken on the role of supporting Mutually Agreed Norms for Routing Security (MANRS), a global initiative that provides crucial fixes to reduce the most common routing threats.

[3] Declaratory Ruling, Order, Report and Order, and Order on Reconsideration In the Matter of Safeguarding and Securing the Open Internet Restoring Internet Freedom, In the Matters of Safeguarding and Securing the Open Internet, WC Docket No. 23-320, and Restoring Internet Freedom, WC Docket No. 17-108 (draft released April 4, 2024), https://docs.fcc.gov/public/attachments/DOC-401676A1.pdf. The core focus of the Declaratory Ruling and Order is, of course, on the question of "network neutrality." A key element of Internet architecture is that user data is relayed throughout the Internet in the form of standardized packets of information without regard for their content, senders, or receivers. This nondiscriminatory approach to Internet traffic is a central premise of the Internet's operation. While there are exceptions—for example, to block packets that are part of a denial-of-service attack—this nondiscrimination is important to protect. We take no position on what legal authority a country should use to implement such protections.

SUMMARY

The Internet Society and the Global Cyber Alliance believe that regulatory mandates about BGP and routing security are unnecessary, will be harmful to routing security in the United States and elsewhere in the world, and will create broader risks to the Internet. Specifically, we will discuss below:

- The United States Internet networks operated by the private sector have made and are continuing to make tremendous strides in improving network security, making a Commission routing security mandate unnecessary.
- A Commission mandate would certainly slow down current progress on routing security during the pendency of the proceeding and any subsequent legal challenges.
- If the Commission were to finalize mandates of routing security actions, networks in the United States would likely then lag behind the global best security practices, which evolve and improve much faster than regulations.
- Depending on the scope of the Commission's mandates, routing regulations could harm the ability of small providers to operate, and lead to network consolidation or lack of access in rural areas.
- Internationally, if the Commission imposes mandated steps on routing security, a range of other countries could follow that example and impose possibly differing and conflicting standards. Having a diversity of global routing security requirements would most likely degrade security and interoperability on the Internet.

With U.S. industry already rapidly deploying Border Gateway Protocol security best practices, and with the harmful impacts that would flow from Commission mandates on routing security, we urge the Commission to step back from and reevaluate possible plans to impose routing security or BGP mandates.

I. The United States industry is already addressing routing security challenges.

While progress on routing security has been historically slow, that has changed significantly in the past few years. The deployment of best practices to secure the routing layer of the Internet—which involves technologies that manage and exchange network reachability information via the Border Gateway Protocol (BGP)—has accelerated dramatically among US industry in the past five years. Industry efforts, including the Mutually Agreed Norms for Routing Security (MANRS) initiative,[4] are leading to better routing security practices among the private sector, not only in the United States but worldwide. In particular, the implementation of one of the most important current routing security technologies, called Resource Public Key Infrastructure (RPKI),[5] improved substantially over the last five years.

[4] *See* https://manrs.org/.

[5] The most widely known application of RPKI is Route Origin Validation (ROV). ROV is a route-filtering process that is executed using Route Origin Authorizations (ROAs), which are cryptographically signed objects that state which Autonomous System (AS) is authorized to originate a particular IP address prefix or set of prefixes. ROV software then verifies the data from trust anchors and, once validated, ROAs can be used to generate route filters.

In the United States, RPKI adoption is increasing at a significant rate among private sector and non-governmental networks. In December 2023, 35.8% of prefixes could be RPKI validated. Between December 2019 and December 2023, RPKI adoption among private sector and non-governmental networks in the United States grew by nearly 350%.

Non-US Federal Networks	# of Valid ROAs	# of Unknown ROAs	# of Invalid ROAs	% Valid ROAs
Dec-19	18754	203528	809	8.406%
Dec-20	35241	206343	684	14.546%
Dec-21	62015	203009	527	23.353%
Dec-22	83238	195207	904	29.797%
Dec-23	103305	184360	874	35.803%

Figure 1Percentage of Route Announcements with RPKI validated prefixes from December 2019 to December 2023, US Non-Federal Networks. Data collected from the MANRS Observatory. See, https://observatory.manrs.org/#/overview.

As highlighted by comments in the Commission's Notice of Inquiry in 2022,[6] the efficacy of RPKI is tied to how widespread its use is. It is also, however, closely tied to the centrality and reach of the network that is deploying it. Given the proliferation of content delivery networks and a smaller number of Internet transit providers, RPKI deployment by these players has a larger impact on routing security than RPKI deployment by "stub networks" (each of which has only one connection to the rest of the Internet). In the United States, despite only a minority of prefixes able to be validated using RPKI in 2022, 58% of traffic went to RPKI-validated routes.[7] At the rate of deployment of route origin validation (ROV) in 2022, RPKI-invalid routes were estimated to have already reduced propagation "by anywhere between one half to two thirds."[8] As the proportion of routes with registered Route Origin Authorizations (ROAs) continues to grow, the effectiveness of techniques like ROV will only increase.

Unfortunately, U.S. Federal Government networks continue[9] to lag behind non-governmental networks in deploying routing security best practices like RPKI. Less than 1% of the routes announced from U.S. Federal Government networks in December 2023 could be RPKI validated (and the poor performance of government networks significantly drags down the overall routing security statistics for the United States).

This process, using ROAs to perform ROV to classify routes as invalid or not, allows networks on the Internet to ignore bad route announcements that are invalid and may be erroneous or malicious in nature.

[6] Notice of Inquiry, In the Matter of Secure Internet Routing, PS Docket No. 22-90 (released Feb. 28, 2022), https://docs.fcc.gov/public/attachments/FCC-22-18A1.pdf ("2022 NOI").

[7] *See* Doug Madory & Job Snijders, *Measuring RPKI ROV adoption with NetFlow*, Apr. 25, 2022, available at https://www.kentik.com/blog/measuring-rpki-rov-adoption-with-netflow/.

[8] *See* Doug Madory & Job Snijders, *How much does RPKI ROV reduce the propagation of invalid routes?*, Aug. 24, 2033, available at https://www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/.

[9] Comments of the Internet Society, 2022 NOI, Mar. 3, 2022, https://www.fcc.gov/ecfs/document/10303534317884/1.

US Federal Gov't Networks	# of Valid ROAs	# of Unknown ROAs	# of Invalid ROAs	% Valid ROAs
Dec-19	9	10645	0	0.084%
Dec-20	11	11218	0	0.098%
Dec-21	12	11525	2	0.104%
Dec-22	63	12507	0	0.501%
Dec-23	108	16610	7	0.646%

Figure 2Percentage of Route Announcements with RPKI validated prefixes from December 2019 to December 2023, US Federal Networks. Data collected from the MANRS Observatory. See, https://observatory.manrs.org/#/overview

In contrast with governmental networks, the deployment of routing security best practices continues to improve among non-governmental United States networks, and the majority of Internet traffic in the United States already enjoys the protections that RPKI validated routes provide. These improvements indicate that network operators are already responding to customer demand, peer pressure, and urging by the Commission, and are moving towards a stronger routing security ecosystem. Given these trends and the dangers to security and the Internet discussed below, the Commission should step back from pursuing routing security regulation.

II. Commission regulation of routing security would slow the strong progress made by the U.S. private sector, and would likely lead the United States to lag behind the rest of the world on routing security.

A Commission regulatory proceeding on routing security would likely harm security both in the short term and the long term.

If the Commission were to proceed with a rulemaking to impose routing security mandates, networks that have not already decided to come into compliance with industry best practices would likely slow routing security investments to see what the Commission ultimately mandates (and whether those mandates survive any legal challenges should they occur). The decision within private corporations to invest in routing security is at times not an easy one, and the prospect of governmental mandates in the area would likely pause forward progress until the mandates are clear. If a Chief Information Security Officer requests corporate support for routing security, they may face the risk of not being able to accurately predict the final requirements of a Commission mandate. This could result in that CISO having to request additional funds to meet the mandate or asking for more funds than necessary to meet the Commission's requirements. Corporate executives who must approve requested funding may choose to simply wait until the mandates are clear. A Commission rulemaking proceeding could easily slow or pause the current progress that we have seen in the United States over the past five years.[10]

[10] *See* WBK Notice of Wireline ISPs Ex Parte Meeting on BGP with Umair Javed, 2022 NOI, Mar. 7, 2023, https://www.fcc.gov/ecfs/document/10215731622834/1 ("[prescriptive regulatory compliance] could diminish security, disrupt operational incident response activities (e.g., with CISA and the Department of Justice/Federal Bureau of Investigation), and undermine U.S. interests in a global, interoperable open Internet. Prescriptive government requirements would do more to freeze or otherwise distort ISPs present security practices than to promote routing security.").

Over the longer term if a Commission-developed mandate was finalized, the Commission's rules would almost certainly set the ceiling of routing security investments by many networks.[11] Some U.S. networks have long been leaders on routing security and we assume that they would continue that leadership, but many other networks would likely simply comply with whatever rules the Commission sets. Networks in the United States would overall fall behind the global best security practices, which evolve and improve much faster than regulations. As noted by Fastly in its response to the 2022 NOI, "enshrining a particular solution as a mandate would likely have other negative effects, such as creating 'tunnel vision' as the community scrambles to comply, limiting the attention and resources needed to develop other approaches and the next generation of tools."[12]

III. Regulating routing security could create barriers to access and incentivize market consolidation.

Implementing routing security best practices is important for improving BGP security. While improving deployment is the ideal, it is important to recognize the challenges deploying some routing security best practices may create for some smaller, less well-resourced networks. Further, as mentioned above, the routing security of small or stub networks will have less impact on the security of the overall routing ecosystem than transit networks or content delivery networks.[13] "Establishing cybersecurity requirements for BGP" or "requiring service providers to deploy solutions to address BGP vulnerabilities," as the Commission mentions in the Declaratory Ruling and Order, could create barriers to entry for small network operators and create new challenges for under resourced networks—particularly those providing last mile connectivity to underserved populations.[14]

In their filing in the 2022 NOI, the Internet Architecture Board (which helps to guide the development of many of the technical standards on which the Internet operates) highlights the importance of the "continuous, modular, flexible evolution of the Internet and its protocols based on operational experience and requirements, where each service provider can determine their security needs based on their diverse requirements and in partnership with other providers."[15] With no single controller, the routing system is difficult to break on a global level, easy to

---

[11] *See*, *e.g.*, Comments of USTelecom–The Broadband Association, 2022 NOI, Apr. 11, 2022, https://www.fcc.gov/ecfs/document/104112779326391/1 ("cybersecurity practices are by their very nature perpetually evolving; today's best-intentioned prescriptive rule would inevitably morph into tomorrow's harmfully outdated compliance box-check").

[12] Reply Comments of Fastly, 2022 NOI, May 10, 2022, https://www.fcc.gov/ecfs/document/10510264496934/1.

[13] *See also* Comments of NTCA–The Rural Broadband Association, 2022 NOI, at 3, Apr. 11, 2022, https://www.fcc.gov/ecfs/document/10411162358102/1.

[14] While the overall routing security of the Internet would be improved if all networks, including small stub networks, adopted routing security best practices, the marginal benefit for the Internet would likely be outweighed by the risk to the ability of small networks to continue to operate (due to the cost of regulatory compliance). But, if the Commission were to adopt a routine security mandate and also exempt small networks, those networks would be even more unlikely to implement these best practices. A better approach for the Commission could be to allow the major networks to continue their forward progress in implementing routing security best practices, and encouraging the development of lower-cost routing security tools targeted at smaller networks.

[15] IAB Comments on A Notice by the Federal Communications Commission on Secure Internet Routing, issued 03/11/2022, 2022 NOI, Apr. 8, 2022, https://www.fcc.gov/ecfs/document/1041122696562/1.

connect to, and it scales well. For small network operators, especially those offering last-mile service in underserved areas, this lack of barriers to connection is crucial. At a time when the United States is investing heavily to connect all Americans, the Commission must proceed cautiously to ensure that small and medium providers—who in many cases may be the only access option in hard-to-reach areas—are not pushed out of the market due to regulatory compliance costs.

As stub networks on the Internet, many of these smaller networks have only one "upstream" provider enabling access to the rest of the Internet. This means that their routing security decisions have minimal effect on the rest of the Internet. At the same time, the relative cost of complying with routing security best practices may be unsustainable for such an operator. For example, small community networks may be run by volunteers and the operators may not have the technical knowledge needed to implement every cybersecurity best practice. For these network operators, who often provide Internet access in areas that the large providers do not serve, and operate on the thinnest of budget margins, the costs of compliance with new BGP security regulations could be problematic, and could threaten their ability to provide services.[16]

IV. Regulating routing security could exacerbate Internet fragmentation and undermine routing security globally.

The Internet routing system is borderless, permissionless, and built on trust among networks. "Improving the security of Internet routing requires individual and collective action on a global scale."[17] However, by introducing regulations regarding BGP security, the Commission threatens to fragment the routing system, undermining the attributes that have made it so successful and weakening routing security. If the United States sets a precedent that a national regulator should impose routing security mandates, then governments around the world are likely to introduce their own routing security rules for network operators. This will force network operators to attempt to comply with competing standards, an impossible task in a traditionally borderless network of networks.

It is easy to connect networks on the Internet because network operators must only adhere to the rules set by the networks with which they agree to exchange traffic. If the Commission and other governments begin creating cybersecurity requirements for network operators, the operators will face a morass of competing requirements to adhere to, and will have to grapple with difficult questions regarding jurisdiction. Would a U.S. network operator that exchanges traffic in Amsterdam with a European network be required to adhere to the Commission's requirements, or to hypothetical future routing security requirements set by the European Union? These are just some of the difficult questions that arise when attempting to apply national regulations to a routing system that is fundamentally and necessarily borderless.

[16] *See* Comments of WTA–Advocates for Rural Broadband, 2022 NOI, Apr. 11, 2022, https://www.fcc.gov/ecfs/document/10411615121646/1.
[17] Comments of Cisco Systems, Inc., 2022 NOI, April 2022, https://www.fcc.gov/ecfs/document/104082196606182/1.

Even more concerning is if routing security rules and standards in some jurisdictions are incompatible with those created by the Commission. Network operators may face barriers to interconnection with networks in other parts of the world, creating the dangers of Internet fragmentation. Actions to politicize connectivity and management of the Internet's infrastructure—regardless of the reason—threaten the Internet and everyone's ability to use it as a resource for good.

There are at least two ways that a Commission-created requirement could inspire such fragmentation. The first, and most obvious, is a case where another government deliberately creates a regulation designed to be incompatible with a regulation created by the Commission. Such a government might indeed be intending to fragment the Internet (or promote a domestically developed standard or technology). Nevertheless, the intentional fragmentation of the Internet would be defended in part on the grounds of national regulation to improve cybersecurity—following the precedent set by this Commission. While as a technical matter such a defense might be dubious, it would nevertheless be harmful to the globally-connected Internet.

The second way, however, is perhaps both more pernicious and more likely. Security specifications are notoriously difficult to write correctly, they benefit from wide review, and are best when they can be updated quickly in light of new security discoveries. It would not be surprising if another jurisdiction adopted regulations that were initially intended to be compatible with Commission requirements. Yet in response to new discoveries, different jurisdictions could respond to those discoveries with different directions at different times, and these could create incompatibilities over time. There is no principled way to avoid this problem, except to recognize that the Internet's routing system is not well-designed for regulation along national lines.

Given the evolution and direction of existing and emerging technologies in routing security, mandates are unlikely to be helpful in securing more networks—and are more likely to "freeze" aspects of an evolving security ecosystem in a damaging manner. Mandates that require certain entities to employ specific routing security measures may seem like a natural solution, but are more than likely to have negative consequences, including potentially taking away momentum from promising new technologies.[18]

[18] We agree with the National Telecommunications & Information Administration, which recommended that:

> the Commission's primary mode of involvement in intricate national security matters should be in partnership with the private sector, and particularly via longstanding multistakeholder processes. The success of initiatives like the Communications, Security, and Interoperability Council (CSRIC), and recent Internet routing security efforts show that these complex issues can be addressed through broad and non-regulatory means, and the Commission should continue to leverage such approaches moving forward.

Ex Parte Comments of the National Telecommunications and Information Administration, Open Internet Proceeding, Mar. 20, 2024, https://www.fcc.gov/ecfs/document/1032004817517/1.

V. Potential Regulation of the Domain Name System

We also briefly note that the Commission's draft Declaratory Ruling and Order states that the Commission might consider regulatory actions to "address security threats related to the Domain Name System (DNS)."[19] We have focused our attention in this document on the threats to security and the Internet itself that could arise if the Commission were to proceed with regulation of routing security, primarily because the Commission had already conducted a Notice of Inquiry concerning routing security. Any suggestion that the Commission might seek to regulate the Domain Name System would raise many similar concerns as discussed above regarding routing security, and in addition could cause extraordinary geopolitical damage to the global consensus that the DNS is administered through a robust multistakeholder process.

CONCLUSION

In such a complex, decentralized global system made up of tens of thousands of individual networks, there is no one "silver bullet" that will make it secure. Regulations to attempt to improve routing security threaten to reduce security, fragment the Internet, and create new barriers to access for users in the United States. As the deployment of routing security best practices continues to rapidly improve among non-U.S. government run networks in the United States, the Internet Society and the Global Cyber Alliance caution the Commission not to try to solve a problem that is already being solved by the broader community.

Respectfully submitted,

INTERNET SOCIETY
Andrew Sullivan, President & Chief Executive Officer
John Morris, Principal, U.S. Internet Policy and Advocacy
Ryan Polk, Director, Internet Policy

GLOBAL CYBER ALLIANCE
Philip Reitinger, President & Chief Executive Officer
Leslie Daigle, Chief Technology Officer & Internet Integrity Program Director

April 17, 2024

[19] Declaratory Ruling and Order ¶ 46.