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

In the Matter of Reporting on Border Gateway Protocol Risk Mitigation Progress	PS Docket No. 24-146

COMMENTS OF THE INTERNET SOCIETY, INTERNET ARCHITECTURE BOARD, AND INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

The Internet Society,[1] Internet Architecture Board,[2] and Internet Corporation for Assigned Names and Numbers (ICANN)[3] submit these comments to respond to the Federal Communication Commission's Notice of Proposed Rulemaking, Reporting on Border Gateway Protocol Risk Mitigation Progress ("NPRM"), and to express our concerns with the potential for negative unintended consequences for the Internet that flow from the NPRM.

---

[1] Founded in 1992 by a number of the original architects of the Internet, the Internet Society is a global charity and 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).

In conjunction the Global Cyber Alliance (GCA), the Internet Society filed comments in a prior proceeding addressing many of the concerns raised here. In this proceeding GCA is filing separate comments more focused on routing security and the value of the Mutually Agreed Norms for Routing Security (MANRS) approach to improving security, and the Internet Society strongly supports those comments as well.

[2] The Internet Architecture Board (IAB) provides oversight of the architecture for protocols and procedures used by the Internet, and also handles the liaison management for the Internet Engineering Task Force (IETF), the main engineering organization that works on standards relating to Internet technology. Its members are listed at https://www.iab.org/about/members/.

The IETF is an open, diverse, and global community of network operators, engineers, researchers and many other stakeholders. The mission of the IETF is "to make the Internet work better" by producing "relevant technical documents that influence the way people design, use, and manage the Internet." The IETF develops, maintains, and evolves the Internet protocol suite and many related standards. The Internet Research Task Force (IRTF) is a closely aligned organization to the IETF with a focus on longer-term research related to the Internet.

[3] The Internet Corporation for Assigned Names and Numbers (ICANN) is a California-based Nonprofit Public Benefit Corporation accountable to a global community of stakeholders. ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifiers that enable the Internet to work. ICANN's wholly-owned affiliate, Public Technical Identifiers (PTI), performs the Internet Assigned Numbers Authority (IANA) functions. These functions include the allocation and assignment of names in the root zone of the Domain Name System (DNS), the coordination of the assignment of Internet protocol parameters and the allocation of Internet numbering resources to Regional Internet Registries. ICANN also facilitates the development and implementation of policies related to the coordination and administration of these unique identifiers to ensure that the Internet remains secure, stable and resilient. The oversight of the IANA functions and the related policy development process take place under ICANN's multistakeholder system of governance.

INTRODUCTION

The global routing system underpins the success of the global Internet. With no single point of failure or single controller, and overseen by a consensus-based multistakeholder process, the routing system is a global and decentralized system based on trust and collaborative decisionmaking. The routing system's key attributes have contributed to the Internet's incredible scalability, flexibility, and overall strength. Routing security has been a historic challenge, but collaborative, non-regulatory efforts in recent years continue to result in significant growth in implementation of routing security best practices, both globally and within the United States.

As we detail below, the Commission's NPRM raises significant concerns not only about harming routing security, but also about undermining the global multistakeholder system and opening the Internet routing system to the threat of fragmentation and government capture. We discuss a number of specific concerns below.

The U.S. Government and the Federal Communications Commission have long supported the multistakeholder model. In a 2012 statement, the Commission itself strongly endorsed the multistakeholder model, and highlighted its value for the Internet:

> The multistakeholder model has enabled the Internet to flourish…. It has ensured the Internet is a robust, open platform for innovation, investment, economic growth and the creation of wealth throughout the world, including in developing countries…. The Internet is a decentralized network of networks and there is **no one party** – government or industry – that controls the Internet today. And that's a good thing.
>
> The Internet's decentralized, multistakeholder processes enable us all to benefit from the engagement of all interested parties. By encouraging the participation of industry, civil society, technical and academic experts, and governments from around the globe, multistakeholder processes result in broader and more creative problem solving. This is essential when dealing with the Internet, which thrives through the cooperation of many different parties….
>
> Our commitment to the multistakeholder model is based on the fact that transparency, inclusion and participation are the 21st century standards governing discussions related to modern communications…. We have and will continue to advocate for an Internet that is not dominated by any one player or group of players, and one that is free from bureaucratic layers that cannot keep up with the pace of change.[4]

Nothing in that 2012 statement is incorrect today. Without the multistakeholder approach, the global Internet would have faced a jumble of competing and conflicting national government regulations. In these comments, we urge the Commission to continue to support the vital

[4] Federal Communications Commission, "The Necessity of an Inclusive, Transparent and Participatory Internet," Nov. 30, 2012 (emphasis in the original), available at https://www.fcc.gov/news-events/blog/2012/11/30/necessity-inclusive-transparent-and-participatory-internet.

foundations of the Internet and to ensure that its actions in this proceeding, in the name of routing security, do not signal to other actors that the building blocks of the Internet are fair game for regulatory capture and competition among countries.

I. The language used and actions proposed by the Commission undermine the multistakeholder model and harm routing security.

The Internet is open, distributed, interconnected, and transnational. The multistakeholder approach to Internet governance provides an accountable, sustainable, and—above all—effective means of decision-making for many institutions that enable the Internet to succeed and thrive.[5] As noted, the United States government has long been one of the strongest supporters of the multistakeholder approach to Internet governance. Unfortunately, the NPRM's minimal discussion of the critical importance of multistakeholder processes to the Internet does little to overcome the Commission's clear interest in taking additional regulatory actions that would undermine the multistakeholder model.

Of greater concern is the NPRM's expansive and top-down regulatory approach, which threatens to undermine key global multistakeholder processes. We highlight two examples from the NPRM below.

A. Expanding the scope beyond last-mile providers, and with more prescriptive regulations, creates risks to the multistakeholder model, and additionally may also harm routing security.

As currently written, the NPRM appears to be limited in its scope of applicability. The requirements in the NPRM are—at least superficially—focused on Broadband Internet Access Service (BIAS) providers (network operators providing last-mile service in the United States), with the more substantial reporting requirements restricted to the largest of these providers.[6] However, several questions the Commission asks in the NPRM seem to reflect an eagerness to expand the groups of network operators covered by the rules or make these rules more prescriptive. Both actions would not only damage the routing security ecosystem in the United States but threaten to fragment the Internet at a more global level. If the United States sets a precedent that a national regulator can and should impose routing security rules on transit providers, then governments around the world are likely to follow suit and consider implementing their own routing security rules for network operators. This would force network operators to attempt to comply with competing and possibly conflicting standards, an impossible task in a traditionally borderless network of networks.

---

[5] Internet Society, "Internet Governance – Why the Multistakeholder Approach Works," Apr. 26, 2016, available at https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.

[6] We believe that even the assessment and reporting requirements in the NPRM are problematic, but in these comments we focus on the language and questions throughout the NPRM that strongly suggest that the Commission wants or perhaps plans to go beyond those requirements both to reach more broadly in terms of coverage and to impose top-down regulations imposing specific actions relating to routing security.

For this reason, limiting requirements to solely BIAS providers–and focusing the rule on purely domestic services—is crucial for ensuring that the impact of the rules is felt domestically and not internationally. If the scope of any potential rules is expanded to apply to transit providers, it is almost inevitable that there will be an extraterritorial reach of the Commission's rules. The Internet is borderless, and many transit providers operate across multiple jurisdictions—even if a network operator may be based in the United States. Applying routing security rules to transit providers would, in effect, force these providers to adhere to U.S. regulations while operating in foreign countries. Such a step starts down the exact path that the global multistakeholder model seeks to avoid: a world in which various governments seek to impose multiple and possibly conflicting rules for technical functions on the global Internet.

This concern is exacerbated by decades-long concerns about U.S. control over the Internet. Over the years, various countries worldwide—both adversaries and allies—have expressed concerns about asserted undue U.S. influence over the governance and operation of the Internet. That was one of many important factors in 2014-2017 that made the "IANA Transition" process (during which the United States formally relinquished any vestige of control over the Internet domain name system) such a critical step to support the global multistakeholder process.[7] Countries continue to be worried when the United States (or other countries) try to enforce their local laws on the global Internet.[8]

Thus, an affirmative decision by a U.S. regulatory agency to regulate internationally the implementation of security technology raises heightened concerns. By imposing U.S. rules on global Internet operations, the Commission would end up encouraging other governments to establish their own regulations for securing Internet routing. Transit providers could quickly find themselves in an untenable position where they have to somehow comply with competing routing security standards imposed by different countries.

Beyond these threats to the multistakeholder model, expanding the rules beyond the basic approach currently laid out in the NPRM could have negative impacts on U.S. network operators and potentially limit the improvement of routing security in this country. Imposing obligations on a broader array of networks could burden networks that are critical for expanding Internet access. At a broader level, potential prescriptive requirements—like Route Origin Validation (ROV) and Route Origin Authorization (ROA) requirements[9]—could harm the development and implementation of new routing security best practices. As mentioned in the Internet Society and Global Cyber Alliance's ex parte filing to the Commission in April 2024, "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."[10]

---

[7] *See, e.g.,* Internet Society, "IANA Transition," 2016, available at https://www.internetsociety.org/iana-transition/.
[8] *See, e.g.,* "Annex 4.2 – Jurisdiction Subgroup – Minority Statement - CCWGAccountability WS2 – March 2018," available at https://www.icann.org/en/system/files/files/ccwg-acct-ws2-annex-4-2-jurisdiction-minority-statement-27mar18-en.pdf.
[9] NPRM ¶¶ 76 and 77.
[10] *See* Ex Parte Comments of the Internet Society and the Global Cyber Alliance, Safeguarding and Securing the Open Internet, WC Docket No. 23-320, and Restoring Internet Freedom, WC Docket No. 17-108, Apr. 17, 2024, available at https://www.fcc.gov/ecfs/document/104170760417493/1. As USTelecom has noted: "Levying top-down rules amid a perpetually shifting threat landscape would countermand the Commission's intention to "spur

Additionally, specific requirements to use ROV and ROAs would, in effect, help freeze the best practices being used by US network operators. As new routing security technologies and best practices are being developed, companies will be less likely to deviate from regulatory-required best practices to implement new technologies. This is particularly challenging if new technologies conflict with existing regulation, but even if new technologies supplement existing regulations, many providers are likely to be slow to move to add new technology because because they are in compliance with existing requirements. And, as future regulation would inevitably lag behind technical changes, this would lead to a risk of the U.S. network operators falling behind network operators in other countries that are able to be more agile in adopting new security technologies.

B. The Commission must avoid interfering with the processes of an RIR.

Regional Internet Registries (RIR) are multistakeholder organizations that oversee the registration and allocation of Internet number resources within a particular region of countries.[11] RIRs develop their policies and processes through a community-driven process from their membership. In a recent rulemaking proceeding, the U.S. Department of Homeland Security (DHS) specifically noted that the American Registry for Internet Numbers (ARIN) was a "multistakeholder organization."[12] Based on that status—*and implementing specific statutory deference to multistakeholder organizations that Congress required*—DHS concluded that ARIN should not be subject to DHS's proposed cybersecurity regulation.[13]

The NPRM seeks comment on processes relating to ARIN, the RIR for the United States, Canada, and many Caribbean and North Atlantic islands, and could be perceived as expressing an interest in impacting those processes.[14] The Commission must be careful not to pursue actions that would impact the multistakeholder processes in RIRs or elsewhere. If the Commission uses regulatory power to influence or regulate ARIN processes, that would undermine the

---

trustworthy innovation for more secure communications and critical infrastructure"; such compliance requirements would stifle rather than promote security innovation, establishing rigid compliance ceilings instead of incenting and ever-rising the floor of evolving best practices." Comments of USTelecom—The Broadband Association, Secure Internet Routing, PS Docket No. 22-90, Apr. 11, 2022, available at https://www.fcc.gov/ecfs/document/104112779326391/1.

[11] Internet Society, "The Internet Ecosystem," 2022, available at https://www.internetsociety.org/wp-content/uploads/2022/07/2022-Internet-Ecosystem-EN.pdf.

[12] "The third group of covered entities that are multi-stakeholder organizations with responsibilities related to the development, implementation, and enforcement of DNS policies are Regional Internet Registries (RIRs). RIRs are multi-stakeholder organizations responsible for managing, distributing, and registering internet number resources (IPv4 and IPv6 address space and Autonomous System (AS) Numbers) within their respective regions. Currently, there are five RIRs in the world: … (3) ARIN, which services the United States, Canada, and many Caribbean and North Atlantic Islands…." Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Docket No. CISA-2022-0010, (May 6, 2024), https://www.govinfo.gov/content/pkg/FR-2024-05-06/pdf/2024-09505.pdf.

[13] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Public Law No. 117-103, Mar. 15, 2022, Division Y, Section 2242(a)(5)(C), available at page 1044, https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf.

[14] NPRM ¶¶ 45, 81.

multistakeholder policymaking system administered by ARIN (in addition to the broader multistakeholder ecosystem under which the Internet operates).

Even if the Commission does not directly pursue actions to influence ARIN's processes, it must still be careful that its actions do not signal to other governments that the United States government is looking to regulate a Regional Internet Registry. This could send a message to governments around the world that they, too, can use regulatory powers to influence RIRs that support the Internet in their regions. That could significantly undermine the global system of IP address allocation.

II. Commission interest in ASPA threatens open standards progress on routing security technologies.

In Paragraph 82 of the NPRM, the Commission highlights several questions it has about Autonomous System Provider Authentication (ASPA), a routing security standard currently being worked on at the Internet Engineering Task Force (IETF).[15] Whether intentional or not, the Commission seems to signal that it is considering imposing top-down routing security regulations, possibly including still-being-developed standards. This could send a serious chill over standards development on routing security.

As the Internet Architecture Board stated in its filing in the Commission's Notice of Inquiry on the Matter of Secure Internet Routing in 2022:

> *The success of future standardization efforts intended to increase routing security, we believe, will be highly dependent on educating BGP users about BGP operational issues and how well real-world deployment experience can be fed back into the multistakeholder standards development process, as opposed to a mandated top-down approach, which would fail to meet the diverse needs of the global community.* [16]

The focus of standards development efforts should be on achieving the best implementable and effective technical solutions. However, in asking about the status of ASPA within the context of an NPRM that floats mandated ROA/ROV requirements, the Commission risks creating perceptions that it is eager to mandate the use of ASPA once it is standardized. Companies may shift their focus in standards development away from creating the best technical standard and towards minimizing future regulation. This would slow down the development of important routing security technologies and the development of new routing security best practices. The Commission's NPRM has already caused concerned discussions within the standards development community.

---

[15] A Profile for Autonomous System Provider Authorization, available at https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/.

[16] IAB Comments on A Notice by the Federal Communications Commission on Secure Internet Routing, issued 03/11/2022, Secure Internet Routing, PS Docket No. 22-90, Apr. 8, 2022, available at https://www.fcc.gov/ecfs/document/104092198205742/1.

Most Internet standards are developed at the IETF, which uses an open standards process composed primarily of engineers and other experts from industry, academia, governments, and civil society. While these experts participate as individuals within the IETF structure, they are often supported to engage in the IETF through support from their employers. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet.[17] As IETF standards are voluntary, there appears to be a willingness from companies to let their engineers engage more freely in this work. If IETF standards being developed are perceived as likely to be mandated by a regulatory authority, such as the concern with ASPA, some companies may alter how they engage to be guided more by a regulatory-impact lens, rather than an engineering centric approach. Currently, the standards development work in the IETF reflects a healthy commitment to achieving the best implementable and effective technical solution to a technical challenge such as security. Any actions that have the effect of undermining that approach to standards would ultimately harm security on the Internet.

The threat that current or future technical standards for routing security would likely become mandated standards would seriously harm the near- and long-term state of routing security, in the United States and across the global Internet.

III. The Commission must proceed very carefully, if at all, on routing security.

As the Commission moves forward in this proceeding, it must ensure that it avoids any actions or implications that could be read to suggest U.S. regulatory interference with the global multistakeholder systems that guide and oversee the Internet.

The Commission must also take care that their actions do not undermine progress already being made by American network operators. In a prior filing by the Internet Society and the Global Cyber Alliance (GCA),[18] we detailed the strong progress that has been made—entirely without regulation—to improve routing security in the United States. We have excerpted a key section of that filing as an Annex to this filing, and we support the GCA's analysis in its filing in this proceeding.[19]

While we do not believe that further action by the Commission is necessary, if the Commission does choose to act, we recommend that the following principles guide its actions:

[17] *See* https://www.ietf.org/about/introduction/.
[18] Ex Parte Comments of the Internet Society and the Global Cyber Alliance, Safeguarding and Securing the Open Internet, WC Docket No. 23-320, and Restoring Internet Freedom, WC Docket No. 17-108, Apr. 17, 2024, available at https://www.fcc.gov/ecfs/document/104170760417493/1.
[19] See Annex A.

- **Limit the scope of covered entities to BIAS providers.** Applying rules to a wider set of providers risks extraterritorial challenges, including conflicting regulations, and could create barriers for small network operators in the U.S.
- **Avoid mandating or appearing to mandate specific security technologies.** Mandating specific security technologies would hold U.S. network operators back from implementing new best practices as they are developed.
- **Lead by example on issues related to legacy address space.** The U.S. Government, like some U.S. network operators, faces serious challenges regarding securing legacy address space.[20] The Government should address its legacy address issues (as it is beginning to do).[21] The Commission should lead by example and support the work of the broader routing security community, including the Mutually Agreed Norms for Routing Security (MANRS) initiative and other stakeholders, to develop effective approaches to the specific challenges facing those networks with legacy address space.

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. As the deployment of routing security best practices continues to improve rapidly in the United States, the Commission must ensure that its actions do not slow this progress and do not threaten the multistakeholder processes that are so essential to the success of the global Internet.

Respectfully submitted,

INTERNET SOCIETY
Ryan Polk, Director, Internet Policy
John Morris, Principal, U.S. Internet Policy and Advocacy

INTERNET ARCHITECTURE BOARD

ICANN
Jamie Hedlund, Senior Vice President Contractual Compliance and U.S. Government Engagement

July 17, 2024

[20] As highlighted by several commenters in the Notice of Inquiry on routing security, network operators with legacy addresses must sign registry services agreements ("RSAs") with the American Registry for Internet Numbers ("ARIN") before being able to implement RPKI. Legacy address space is IPv4 address space which was distributed before the establishment of the RIR System. As noted by several stakeholders, signing an RSA with ARIN can be a challenge for network operators with significant legacy address space, including government agencies.

[21] *See* U.S. Department of Commerce, "U.S. Department of Commerce Implements Internet Routing Security" May 2024, available at https://www.commerce.gov/news/press-releases/2024/05/us-department-commerce-implements-internet-routing-security.

Annex A

EXCERPT FROM

Ex Parte Comments of the Internet Society and the Global Cyber Alliance in the Matter of Matter of Safeguarding and Securing the Open Internet, Restoring Internet Freedom

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

Apr. 17, 2024
https://www.fcc.gov/ecfs/document/104170760417493/1.

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,[22] 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),[23] improved substantially over the last five years.

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%.

[22] https://manrs.org/.

[23] 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. 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.

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,[24] 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.[25] 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."[26] 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[27] 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).

[24] 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").
[25] *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/.
[26] *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/.
[27] 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, 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.