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
	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90

To: The Commission

JOINT REPLY COMMENTS OF
NTCA–THE RURAL BROADBAND ASSOCIATION AND
WISPA – THE ASSOCIATION FOR BROADBAND WITHOUT BOUNDARIES

NTCA–The Rural Broadband Association ("NTCA") and WISPA – The Association for Broadband Without Boundaries ("WISPA") ("the Associations") hereby reply to the initial comments submitted in response to the Notice of Proposed Rulemaking ("*Notice*")[1] adopted by the Commission in the above-captioned proceeding.

A majority of commenters share the Associations' concern that the proposals in the *Notice* exceed the Commission's authority, would impose burdens on Broadband Internet Access Service ("BIAS") providers without a commensurate increase in internet routing security, and would substitute the Commission's cybersecurity policy choices for BIAS providers' own, successful, risk-based analysis – all to the detriment of the agency's stated goal. Should the Commission conclude that it has authority to adopt rules subjecting BIAS providers to Border Gateway Protocol ("BGP") requirements, the Commission must be mindful of the financial and

[1] *Reporting on Border Gateway Protocol Risk Mitigation Progress*, Notice of Proposed Rulemaking, PS Docket Nos. 24-146, 22-90, FCC 22-18 (rel. June 7, 2024).

operational challenges, risks and burdens that new mandatory obligations would place on BIAS providers, especially smaller providers that may lack the resources to comply.

I. COMMENTERS AGREE THE COMMISSION DOES NOT HAVE STATUTORY AUTHORITY TO IMPLEMENT THE PROPOSED REGULATIONS.

Multiple commenters support the Associations' assessment that the Commission lacks authority to regulate BIAS providers' internet routing security practices.[2] The Commission's reliance on Title II of the Communications Act of 1934, as amended (the "Act"), is misplaced and, in any event, would be applied prematurely pending resolution of legal challenges to the *2024 Open Internet Order*.[3] The Associations further support CTIA's conclusion that, even if the *2024 Open Internet Order* were upheld, Title II would not provide the Commission with authority to regulate BGP because: (1) the statutory definition of "telecommunications service" does not encompass BGP security; and (2) Sections 201 and 202 of the Act do not grant the Commission authority over BGP routing or security, nor could those statutes be considered broad enough grants of authority for the Commission to regulate in the cybersecurity space.[4] Outside

[2] *See* Joint Comments of NTCA – The Rural Broadband Ass'n and WISPA – The Ass'n for Broadband Without Boundaries, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 15-17 ("Joint NTCA and WISPA Comments"); Comments of ACA Connects, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 6-7 ("ACA Connects Comments"); Comments of CTIA-The Wireless Ass'n, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 15-34 ("CTIA Comments"); Comments of USTelecom – The Broadband Ass'n, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 35-46 ("USTelecom Comments").

[3] *Safeguarding and Securing the Open Internet*, WC Docket No. 23-320, FCC 24-52, Ruling, Order, Report and Order, and Order on Reconsideration, at ¶¶ 28-29 (rel. May 7, 2024) ("*2024 Open Internet Order*"); Joint NTCA and WISPA Comments at 15-16; ACA Connects Comments at 6-7; CTIA Comments at 18-21.

[4] *See* CTIA Comments at 18-21.

of Title II, neither Section 303(b) of the Act[5] nor Section 706 of the Telecommunications Act of 1996[6] provides the Commission with the requisite authority to regulate BGP.[7]

The Associations further agree with CTIA and USTelecom that the Communications Assistance for Law Enforcement Act ("CALEA") likewise does not authorize the Commission to impose BGP mandates.[8] CALEA does not provide broad security powers that would authorize the Commission to regulate BIAS providers' cybersecurity.[9] The *Notice* cites Section 105 of CALEA, the Security and Integrity ("SSI") provision, which requires telecommunications providers to prevent unauthorized interceptions.[10] The provision, though, is specifically targeted to protect lawful interceptions authorized under CALEA, and is not a larger mandate for broader security measures.[11] Moreover, CALEA specifically prohibits law enforcement agencies from requiring "any specific design of equipment, facilities, services, features, or system configurations."[12] The Commission's proposed mandating of Resource Public Key Infrastructure ("RPKI") would violate that prohibition.[13] Lastly, CALEA only allows the Commission to set technical standards if industry associations fail to do so.[14] That is not the case here, as industry associations have already issued multiple technical requirements and standards.[15]

[5] 47 U.S.C. § 303(b).

[6] 47 U.S.C. §1302.

[7] *See* Joint NTCA and WISPA Comments at 16-17; CTIA Comments at 21-26; USTelecom Comments at 39-41.

[8] *See* CTIA Comments at 27-29; USTelecom Comments at 42-44.

[9] *See id.* at 26-27.

[10] 47 U.S.C. § 1004.

[11] *See* CTIA Comments at 27; *see also* USTelecom Comments at 43.

[12] *See, e.g.,* 47 C.F.R. §§ 1.20003, 1.20004, 1.20005.

[13] *See* CTIA Comments at 28; *see also* USTelecom Comments at 43.

[14] 47 U.S.C. § 1006(b).

[15] *See* CTIA Comments at 29; *see also* USTelecom Comments at 44.

For all the foregoing reasons, the Commission's reliance on CALEA as authorization for imposing BGP mandates is flawed.

At best, the Commission relies on questionable authority, and at most relies on authority subject to pending judicial challenges. Accordingly, the Commission should not move forward with the proposals in this proceeding until the courts have resolved all challenges to the *2024 Open Internet Order*.

II. COMMENTERS AGREE THAT THE COMMISSION SHOULD AVOID IMPOSING BURDENSOME REQUIREMENTS THAT MAY HAVE A LIMITED IMPACT ON INTERNET ROUTING SECURITY AND THAT RISK ONGOING CYBERSECURITY INITIATIVES.

Multiple commenters expressed substantial concerns regarding the breadth and lack of clarity of the Commission's proposals, in part because these are targeted toward a small portion of the overall internet ecosystem. NTIA, for example, along with the Associations, pointed out that imposing BGP requirements solely on BIAS providers would have little impact on the internet as a whole, whereas requiring the federal government to register ROAs for the IP prefixes held by each agency or department would have the most significant impact on routing security.[16] As numerous commenters demonstrated, BIAS providers handle a very small portion of internet traffic and many of these providers do not even route traffic themselves but rather simply connect end users to a transport provider – which often is not a BIAS provider – from which the traffic is then carried across the internet. USTelecom, for example, pointed out "the

[16] Comments of NTIA, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024) ("NTIA Comments"), at 9 ("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."); *see also*, *id*. at 12 ("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."); *see also id*. at 13 ("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.").

ISPs that provide BIAS are only one part of the global internet routing ecosystem. They are not the only [Autonomous System ("AS")] operators: large companies, universities, and government agencies, among other organizations, also operate AS's and control IP addresses."[17] As a result, imposing internet routing requirements on this select group simply because the Commission has claimed authority to regulate BIAS providers would at most have a minimal impact on internet routing security, while imposing costly financial and operational burdens on this select group of entities. This is especially true with respect to smaller BIAS providers.

Instead of imposing far-reaching requirements that may have at best a minimal impact on internet routing security, and that could cause harm if designed improperly or if utilized in lieu of other cybersecurity practices, the Commission can, as NTIA recommended, "improve BIAS provider security and prevent routing incidents" through a "narrow and targeted" reporting requirement focused on ROA adoptions.[18] While the Associations agree that secure internet routing can play a role in BIAS providers' overall cybersecurity strategy, BIAS providers should not be required to either create a separate plan detailing their internet routing strategy or amend existing cybersecurity plans to include such information.[19]

The Commission can better accomplish the *Notice*'s objective by engaging with ONCD to raise awareness among private entities and other federal agencies of the role ROAs play in securing internet routing and by helping eliminate obstacles to ROA registrations. The Associations further support NCTA's recommendation that the Commission minimize any reporting requirement by utilizing publicly available information to identify trends in ROA

[17] USTelecom Comments at 11.

[18] NTIA Comments at 12.

[19] *See* Comments of T-Mobile, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 9.

adoption across the entire internet ecosystem.[20] With this awareness, the Commission can more effectively work with ONCD and other federal agencies to increase awareness of, and reduce roadblocks to, ROA adoption in those areas.

III. COMMENTERS RECOMMEND THE COMMISSION MAINTAIN AND SUPPORT A COLLABORATIVE MULTI-STAKEHOLDER APPROACH.

The Commission's proposed rules would mandate that BIAS providers – regardless of size or amount of Internet routing performed – not only implement secure internet routing but also that such routing be carried out using RPKI in lieu of other methods. Such a mandate would fail to account for the needs and capabilities of small BIAS providers and supplant the Commission's overarching policy judgment for each provider's tailored risk-based assessment of the cyber practices best suited for their network and capabilities.

Imposing prescriptive regulatory requirements also risks undoing the important public-private approach that provides flexibility for both the government and industry to adapt over time to new technologies and threats – an approach expressly encouraged by ONCD.[21] As several commenters noted, the collaborative approach between the government and BIAS providers over the past several years has led to increased adoption of secure internet routing methods as well as other important cybersecurity initiatives.[22] Significantly, the National Institute of Technology

[20] NCTA Comments at 12.

[21] *See* Memorandum for the Heads of Executive Departments and Agencies from Office of Management and Budget, Jul. 10, 2024, at 3 ("regulatory agencies are strongly encouraged to consult with regulated entities to establish baseline cybersecurity requirements that can be applied across critical infrastructure sectors but are agile enough to adapt as adversaries increase capabilities and change tactics."), https://www.whitehouse.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf.

[22] *See* Comments of NCTA – The Internet & Television Association, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 8 ("… the Federal government has advanced cybersecurity improvements through collaborative, risk-and consensus-based measures and best practices in botnet prevention, supply chain risk management, critical infrastructure security, secure software development, and IoT device

("NIST") Cybersecurity Framework 2.0 ("CSF"), as well as predecessor versions, is a product of ongoing collaboration between industry and NIST and was expressly designed to be adapted to the specific needs and capabilities of each entity.[23]

Both the Cybersecurity and Infrastructure Security Agency ("CISA") and the Commission have repeatedly and successfully used public-private collaboration to develop expert guidance on critical cybersecurity and supply chain topics through the Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force and the Communications Security, Reliability, and Interoperability Council ("CSRIC").[24] NTIA similarly advised the Commission that "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]

---

standards.") ("NCTA Comments"). *See also* ACA Connects Comments at 3 ("ACA Connects encourages the Commission to … maintain and support the multi-stakeholder collaborative approach that has created success in the cybersecurity space.").

[23] *See, e.g.*, NIST Seeks Input to Update Cybersecurity Framework, Supply Chain Guidance (Feb. 22, 2022), https://www.nist.gov/news-events/news/2022/02/nist-seeks-input-update-cybersecurity-framework-supply-chain-guidance; *Views on the Framework for Improving Critical Infrastructure Cybersecurity*; Request for Information, 80 FR 76934 (rel. Dec. 11, 2015); The NIST Cybersecurity Framework (CSF) 2.0 (Feb. 26, 2024), at 1 ("The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes."), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[24] *See* ICT Supply Chain Risk Management Task Force ("Composed of federal government and industry representatives from across the Information Technology and Communications Sectors, the Task Force serves as the Agency's center of gravity for supply chain risk management partnership activity."), https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force; *FCC Announces Intent to Re-establish the Communications Security, Reliability, and Interoperability Council, and Solicits Nominations for Membership*, Public Notice, DA 23-1187 (rel. Dec. 20, 2023) ("In seeking nominations for CSRIC IX, Chairwoman Rosenworcel will again look to include in the Council's membership [] a broad variety of stakeholders, including representation from the FCC's federal government partners with similar interests.").

[25] NTIA Comments at 8.

In lieu of new, burdensome regulations targeted only at BIAS providers, the Associations support other commenters and encourage the Commission to continue engaging with all internet stakeholders, both public and private, to build upon the increase in internet routing security that has already taken place.[26] A collaborative approach to internet security that incorporates a wide swath of private-sector and government entities will have a far greater impact on achieving the Commission's goals than broad regulations that apply only to BIAS providers and that threaten innovation and expansion.[27] Furthermore, this approach can take into account, and address specifically, the challenges confronting both public and private sector entities, thereby enhancing internet routing security rather than penalizing BIAS providers who are unable to comply with Commission regulations due to these obstacles. To successfully build upon the broad strides BIAS providers have already achieved with respect to internet routing security, the Commission should work with other federal agencies to encourage and support ROA registrations by federal agencies as well as other AS operators.[28]

Numerous commenters also oppose the Commission's proposal to adopt rules that would require BIAS providers alone to implement RPKI specifically rather than continuing to engage in the collaborative industry-wide approach successfully undertaken for both secure internet routing

[26] *See* NTIA Comments at 5-8; ACA Connects Comments at 3; CTIA Comments at 6-8; Comments of INCOMPAS, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 2; Comments of Internet Society, Internet Architecture Board, and Internet Corporation for Assigned Names and Numbers (ICANN), PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 3-5; NCTA Comments at 8-9.

[27] NTIA Comments at 8 ("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.'"); USTelecom Comments at 12 ("Regulation in this context would needlessly impede our nation's ability to marshal private sector cybersecurity talent effectively and dynamically.").

[28] *See* CTIA Comments at 11-12; ACA Connects Comments at 3 (citing National Cybersecurity Strategy Implementation Plan, Initiative 4.1.5); CTIA Comments at 8; Comments of Cisco Systems, Inc., PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 8.

and cybersecurity practices generally. As Internet2 and The Quilt pointed out, "[r]outing security is a relatively new framework and is evolving rapidly. Any regulation that identifies a specific routing security technology runs the risk of hindering the advancement of evolving technical solutions."[29]

In contrast to supporting a flexible and inclusive, multi-stakeholder approach, the Commission's industry-specific proposals are overly burdensome and risk stifling technological advancements. Imposing internet routing requirements upon BIAS providers specifically could also lead to unintended and harmful consequences that would fall especially hard on small BIAS providers due to their limited financial and personnel resources. NTIA echoed this concern, stating that "[s]mall networks have limited resources and staff" and emphasized that "[r]outing security should not be a zero-sum game where gains in routing security come at the cost of other priorities."[30]

The Commission's proposal to mandate a certain threshold for ROA registrations could be especially harmful to small BIAS providers because in certain circumstances, the cost and complexity of registering ROAs in some instances may exceed some BIAS providers' capabilities. For instance, while ARIN confirmed owners of reassigned address spaces are unable to perform ROA registrations using ARIN's Hosted RPKI service, ARIN also commented that "providers running their own CA using ARIN's Delegated RPKI service may choose to develop and provide their customers with this capability for their reassigned address space."[31] Doing so, however, requires significant time and technical expertise. As a result, small BIAS

[29] Comments of Internet2 and The Quilt, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 7.
[30] NTIA Comments at 13-14.
[31] Comments of ARIN, PS Docket Nos. 24-146, *et al.* (filed Jul. 17, 2024), at 2.

providers are unlikely to be able to avail themselves of this option as "networking engineers who are routing experts are in limited supply."[32] Therefore, if the Commission were to mandate a certain ROA adoption threshold, small BIAS providers who use reassigned IP addresses would be at risk of noncompliance with the Commission's rules. Clearly, this outcome does not benefit anyone and could lead to the provider concluding the cost of complying with the Commission's BGP rules, compounded with the numerous other requirements imposed by the Commission recently, is unfeasible.[33] At a time when the Commission, Congress, and other federal agencies are working hard to expand broadband access to rural areas, developing rules that could drive existing BIAS providers to discontinue their operations is clearly not in the public's best interest.

IV. CONCLUSION

Based on the foregoing, the Associations recommend that the Commission refrain from imposing regulations mandating secure internet routing and instead continue engaging with public and private sector stakeholders to develop risk-based strategies for internet routing security that are adaptable to changes in technology, threats, and each entity's needs and capabilities.

Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Tamber Ray
NTCA – The Rural Broadband Association
4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203

By: */s/ Louis Peraertz*
Louis Peraertz
WISPA – The Association for Broadband Without Boundaries
200 Massachusetts Ave., NW
Suite 700
Washington, DC 20001

[32] CTIA Comments at 42.

[33] *See* Joint NTCA and WISPA Comments at 10. *See also* USTelecom Comments at 20.