Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 26-82
Threats in Domestic Telecommunications	)	
Service	)	

COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION

By: */s/* Justin Faulb
Justin Faulb
Tamber Ray
Brian Ford
4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203
703-351-2000 (Tel)

June 8, 2026

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 26-82
Threats in Domestic Telecommunications	)	
Service	)	

COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION AND SUMMARY

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Notice of Proposed Rulemaking issued by the Federal Communications Commission ("Commission") in the above-captioned proceeding.[2] In the *Notice*, the Commission proposes for the first time to prohibit entities deemed a threat to national security from providing domestic interstate telecommunications service pursuant to blanket authority under section 214 of the Communications Act of 1934, as amended (the "Act") and to limit telecommunications carriers' ability to interconnect with such entities.[3]

NTCA and its members strongly support the Commission's goal of protecting the nation's communications networks from national security threats. Indeed, NTCA's Small

[1] NTCA represents approximately 850 community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[2] *Protecting Against National Security Threats in Domestic Telecommunications Service*, Notice of Proposed Rulemaking, WC Docket No. 26-82 (May 1, 2026), 91 Fed. Reg. 25325 ("*Notice*").

[3] The Commission maintains a list ("Covered List") of communications equipment and services deemed to pose "an unacceptable risk to the national security of the United States" pursuant to the Secure and Trusted Communications Networks Act of 2019 ("Secure Networks Act").

Broadband Provider ISAC, CyberShare, promotes the resiliency and continuity of operation of small network operators across the United States.[4] NTCA also participates on a number of collaborative national security partnerships with fellow carriers and the United States government.

As the Commission considers whether to expand use of the Covered List to restrict domestic section 214 services, as well as interconnection between carriers and certain facilities, NTCA urges the Commission to take great care to ensure that any actions are targeted to protect against specific and identifiable risks, and narrowly tailored to ensure that domestic broadband providers are not harmed when complying with the Commission's restrictions. The Commission should also ensure any actions taken in this proceeding do not block lawful communications permitted by U.S. law and are clearly defined to avoid confusion. Such actions are necessary to avoid placing carriers in the precarious position of blocking traffic for fear of being found in violation of Commission rules while at the same time risking harm to U.S. businesses whose communications have been disrupted.

Considering the likely implications of the *Notice's* proposals on restricting and limiting both the availability and feasibility of direct interconnection, NTCA urges the Commission to harmonize any rules adopted in this proceeding that could impact interconnection with the Commission's ongoing proceedings related to transitioning interconnection to all-Internet Protocol ("IP"). Interconnection is complicated and is poised to undergo a major regulatory

[4] *See* CyberShare: The Small Broadband Provider ISAC ("CyberShare collects and disseminates threat information, indicators and mitigation strategies from a variety of public and private sources and facilitates communications among participants."), *available at* www.cyber-share.org (last visited June 2, 2026).

evolution via a pending proceeding.[5] As NTCA members and the industry as a whole continue to transition toward all-IP interconnection, adding additional barriers to interconnection including uncertainty as to which entities or facilities may or may not be acceptable interconnection partners could negatively harm access to connectivity.

If the Commission chooses to adopt rules prohibiting certain interconnection arrangements, as proposed in the *Notice*, the Commission should ensure that (i) carriers can rely upon reasonable representations from interconnecting partners that they are authorized to provide the offered services, (ii) the rules provide a suitable transition period to avoid harm to consumers, and (iii) any prohibitions based on updates to the Covered List only apply prospectively. At a minimum, the Commission should limit any prohibitions on interconnections to parties identified by name on the Covered List and avoid expanding the universe of covered entities to those owned, controlled, or subject to the jurisdiction of a foreign adversary.

II. INTERCONNECTION IS A VITAL ASPECT OF NETWORK MANAGEMENT AND ANY ACTIONS HERE SHOULD ALIGN WITH OTHER IP INTERCONNECTION PROCEEDINGS

NTCA supports the Commission's long-standing goals of both "protecting our communications networks against foreign threats"[6] and ensuring an ordered and seamless transition to all-Internet Protocol ("IP") interconnection. Communications providers do not operate in isolation, however. Voice, Internet, video, transport, cloud services, and security tools all depend on interconnection with other providers and vendors. As such, we urge the Commission to ensure that any prohibitions to the domestic section 214 interconnection regime

[5] *Advancing IP Interconnection*, WC Docket No. 25-304, *Accelerating Network Modernization*, WC Docket No. 25-208, *Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Proposed Rulemaking, FCC 25-73 (Oct. 29, 2025).

[6] *Id*. at ¶ 1.

do not inadvertently undermine connectivity amid the nation's complex transition to all-IP interconnection. Specifically, the Commission should avoid any changes to the domestic section 214 rules that would jeopardize carriers' ability to understand which entities they are legally allowed and required to interconnect with, and which impose significant cost increases without a commensurate national security benefit.

Broadband providers are working with the Commission and across the connected ecosystem to evolve the existing interconnection framework to promote an industry-wide transition to IP-based interconnection.[7] That proceeding will produce the most comprehensive, wholesale changes to the Commission's interconnection rules since the agency's implementation of the Telecommunications Act of 1996.[8] The ultimate resolution of the open IP interconnection proceeding will have significant implications for how providers exchange voice traffic and manage their networks, as well as how interconnection is managed to protect national security, public safety, and consumers.

Proposals contained in the *Notice* could directly impact and complicate this transition. For example, prohibiting interconnection with entities or facilities with equipment from entities on the Covered List – including "current and future affiliates and subsidiaries and any entity included by reference therein" – may eliminate significant Points of Presence ("PoPs") from U.S. networks, raising costs and limiting service routes that facilitate American connectivity. Expanding the Commission's rules to prohibit entities owned or controlled by, or subject to the jurisdiction or direction of a foreign adversary from providing interstate telecommunications

[7] *See id*., fn. 5.

[8] *See Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*, CC Docket Nos. 96-98, *Interconnection between Local Exchange Carriers and Commercial Mobile Radio Service Providers*, 95-185, First Report and Order, FCC 96-325 (Aug. 8, 1996).

service pursuant to domestic section 214 authority would exacerbate the problem by creating significant uncertainty for all broadband providers and facilities regarding whom to interconnect with and how to deliver traffic. This could delay interconnection, limit availability to services, and harm consumers. This burden would be more substantial for smaller and rural providers with fewer resources to vet interconnection points and increase costs as they have to find new interconnection partners or facilities and negotiate agreements. The *Notice*'s proposal to prohibit telecommunications providers from interconnecting with such entities, or facilities that have deployed equipment from a covered entity, would have the same effects.[9]

The novel approach, questionable authority, and implications contained therein, counsel caution in this proceeding to avoid unintended consequences that could negatively implicate connectivity to Americans. The Commission's authority to act is uncertain and would be more secure by adhering to established processes set forth in the Secure and Trust Communications Networks Act of 2019 ("Secure Networks Act")[10], rather than relying upon Title II authorities as a potential new source of authority.

How providers interconnect – whether direct or indirect, over the public Internet, or through "cloud-based" platforms, as well as how such interconnection can be achieved while protecting consumers,[11] should be determined on a holistic basis rather than piecemeal in competing proceedings. The Commission should also ensure that any actions taken are narrowly tailored and limited to protecting against specific and identifiable risks while at the same time

[9] *Notice* at ¶ 15.

[10] Pub. L. No, 116-124, 134 Stat. 158 (2020).

[11] *See* Comments of NTCA–The Rural Broadband Association, WC Docket Nos. 25-304, 25-208 & 17-97 (Jan. 20, 2026), p. 14 (advocating for a "light-touch IP interconnection framework that safeguards the proper routing of calls (including critical public safety calls) and preserves the affordability of voice service for rural consumers before the existing construct is torn down").

targeted to ensure that domestic broadband providers are not harmed by complying with the Commission's restrictions. Thus, while protecting the nation's communications networks from national security is paramount, the Commission can and should address this on as narrow a basis as possible in this proceeding. Otherwise, creating overly broad rules excluding carriers that don't pose a threat could harm all Americans by making it more difficult to understand exactly where vulnerabilities exist in networks by throwing the good out with the bad, and harming IP interconnection in the process. Finally, the scope of any prohibition the Commission may enact here is not defined. More specifically, the *Notice* fails to indicate whether any prohibited connections with other entities would extend beyond formal interconnection agreements and include peering, transit arrangements, cloud services, or even connections to content delivery networks. At the very least the Commission invites confusion and at worst broad restrictions could undermine the provision of all kinds of services to consumers.

III. ANY PROHIBITION SHOULD BE LIMITED TO NAMED ENTITIES ON THE COVERED LIST AND SHOULD NOT EXPAND COVERED ENTITIES TO THOSE OWNED, CONTROLLED, OR SUBJECT TO THE JURISDICTION OF A FOREIGN ADVERSARY

The Commission proposes wide-ranging prohibitions on telecommunications carriers' ability to interconnect with entities named on the Covered List and seeks comment on whether to expand those prohibitions to entities owned, controlled, or subject to the jurisdiction or direction of a foreign adversary. The Commission should limit any prohibitions to those entities explicitly identified by name in the Covered List.

Due to the complex nature of domestic telecommunications networks, expanding the prohibition to include entities that are owned, controlled, or subject to the jurisdiction or direction of a foreign adversary could result in an overbroad prohibition that requires a significant reorganization of networks and routing of voice and data traffic. Without an explicit

determination that a particular entity poses a threat to national security pursuant to the process identified in the Secure Networks Act, the Commission's proposed actions could be so widespread as to severely limit carriers' options for interconnecting providers. This could in turn harm consumers if providers are forced to route data traffic through congested alternative interconnection routes or if they are forced to carry voice or data traffic to distant points to find an interconnection partner. This is particularly a concern for small, rural carriers that are typically based in geographically isolated communities as these providers may have few if any alternatives for routing voice and/or data traffic. Accordingly, the harm from removing a provider from the domestic network would outweigh any benefit, absent a true risk to national security.

The Commission proposes to rely upon section 214 of the Act as authority for excluding entities identified on the Covered List from providing domestic interstate telecommunications services.[12] Section 214, however, expressly applies to telecommunications carriers, as the Commission recognized.[13] Any attempts to restrict telecommunications carriers' ability to interconnect with non-telecommunications carriers, such as PoPs and data centers, therefore cannot be based on section 214 alone and instead must be considered in coordination with established methods used by the United States government for protecting national security. For the same reason, the Commission should reject the *Notice's* proposal that would prohibit carriers from interconnecting with facilities – such as unlicensed fixed wireless equipment, PoPs, and data centers – that are owned, controlled, or subject to the jurisdiction or direction of a foreign adversary, or that may have deployed Covered List equipment. Prohibiting carriers from

[12] *Notice* at ¶ 1.

[13] *See id.* at n. 28.

interconnecting with unlicensed fixed wireless services, PoPs, and data centers without a clear determination of risk to national security would impose a significant burden on small carriers and could harm consumers by cutting off access to locations or services upon which they rely.

The Commission implicitly recognizes in the *Notice* that access to data centers and PoPs is vital by suggesting that owners/operators of such facilities could seek a waiver of the requirements or have "limited connectivity."[14] Simultaneously adopting a rule requiring carriers to identify whether connecting with any given PoP or data center is permissible under the Commission's rules while also allowing for the possibility that any given PoP or data center could obtain a waiver of the prohibition would add further burden and confusion on carriers with little to no added benefit.

To minimize the burden and provide clarity, if the Commission chooses to restrict telecommunications carriers' ability to interconnect with entities identified on the Covered List, such restrictions should apply solely to formal interconnection arrangements while also providing an opportunity for entities to cure their defect and allow carriers to interconnect. This is consistent with Commission precedent[15] and would reduce harm to consumers caused by interrupted services.

The alternative, where the Commission simply adopts all of the *Notice*'s proposals, would be unworkable for small and rural carriers. Small and rural carriers do not have the ability to identify the ownership structure of entities they interconnect with, nor can they affirmatively

[14] *Notice* at ¶ 14.

[15] *See, e.g.*, *China Unicom (Hong Kong) Operations Limited*, Order, DA 25-1021 (EB Dec. 8, 2025) (directing China Unicom (Hong Kong) to cure deficiencies in its Robocall Mitigation Database certification). The Commission allows providers the opportunity to cure a deficiency before taking more drastic steps, such as removing a provider's certification from the Robocall Mitigation Database. *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2604, ¶ 60 (2023).

ascertain whether an entity is "owned, operated, or subject to the jurisdiction or direction of a foreign adversary." Furthermore, the list of foreign adversaries itself is subject to change without notice and is effective immediately. As a result, under the Commission's proposal, carriers would be expected not only to be aware of changes in the list of foreign adversaries but also to somehow know whether any given entity is "owned, operated or under the jurisdiction or direction of" a foreign adversary all while the prohibition would be effective immediately, absent a waiver which may or may not be pending.[16] This would in turn require small providers with limited staff resources to reroute traffic immediately. Such "dynamic" changes to interconnection agreements and routing practices are likely beyond the means of most providers, much less small entities.

IV. ANY PROHIBITION MUST AVOID INTERRUPTING THE DELIVERY OF TELECOMMUNICATIONS SERVICES AND PROVIDE MEANS FOR PROVIDERS TO COMPLY WITH NEW RESTRICTIONS

NTCA urges the Commission to empower all carriers, but especially small and rural carriers, to comply with any prohibition in the least burdensome manner. The Commission should also keep in mind that the United States government has a variety of tools available outside of the Covered List and domestic section 214 authorization to secure communications networks. Additionally, before acting here, the Commission should leverage partnerships with industry to effectively address national security risk while also minimizing harm.[17] These

[16] *See, e.g.*, 15 C.F.R. § 791.4(b) ("the list of foreign adversaries will be revised as determined to be necessary. Such revisions will be effective immediately upon publication in the Federal Register without prior notice or opportunity for public comment.").

[17] For instance, the Commission established the Communications Security, Reliability, and Interoperability Council ("CSRIC"), which includes representatives from the private sector, state, local and tribal government agencies, and the federal government, to provide recommendations that would enhance the security, reliability, and interoperability of communications systems. The Communications Information Sharing and Analysis Center (COMM-ISAC) also partners with private entities and government agencies to share threat information relevant to communications infrastructure.

longstanding partnerships are often more effective than broad prohibitions at targeting and mitigating threats.[18]

In the event the Commission does move forward, carriers should be allowed to rely upon reasonable representations from interconnecting providers that the providers do not violate the Commission's rules. The Commission should also allow sufficient time to transition from a covered interconnected carrier or facility if necessary due to national security and ensure any rules are prospective.

A. Carriers Should be Able to Rely on Reasonable Representations

To ensure any actions taken by the Commission in this proceeding are the least restrictive possible, the Commission should allow entities authorized to provide domestic interstate telecommunications service pursuant to section 214 blanket authority to rely upon reasonable representations by PoPs, data centers, fixed wireless equipment, or others with whom they offer or are considering offering interconnection services with respect to their domestic section 214 authorization, use of equipment identified on the Covered List, and the company's ownership, including whether the entity is owned, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Absent authorization to rely upon such representations, small carriers already stretched thin in terms of financial and staff resources would be forced to expend time and resources attempting to obtain information that may be difficult, if not impossible, to acquire. Small carriers are already challenged to comply with frequent changes to the Covered

[18] *See, e.g.*, Statement of Chairman Brendan Carr, *Protecting the Nation's Communications Systems from Cybersecurity Threats*, Order on Reconsideration, PS Docket No. 22-329 (Nov. 21, 2025) ("the FCC has worked directly with carriers who have agreed to make extensive, coordinated efforts to harden their networks against a range of cyber intrusions. These have included accelerated patching of outdated or vulnerable equipment, updating and reviewing access controls, disabling unnecessary outbound connections, improving their threat-hunting efforts, and increasing cybersecurity information sharing. All of these actions have been well within FCC legal authority and have effectively mitigated network vulnerabilities.").

List while also ensuring supply chain delays caused by such changes do not interfere with their ability to continue expanding services and to replace end-of-life equipment.[19] This would be an additional burden.

In addition, resources to do so aside, small entities such as those represented by NTCA simply do not have the ability to ascertain the ownership structure of these types of equipment/facilities or whether they are operating under the guise of a foreign adversary. Carriers or facilities may have confidential or non-disclosure agreements with their vendors or may reasonably want to limit the details they share with interconnecting carriers for a variety of reasons. Carriers of all sizes also have no control or awareness over the equipment third parties deploy or any ability to identify what equipment is deployed outside of their purview, including when equipment installed in these facilities is replaced or updated, or the provenance of such equipment. Placing burdensome and unworkable obligations on small carriers could make compliance with the Commission's rules unachievable.

B. Carriers Must Have Time to Find New Interconnection Pathways

The Commission must provide carriers with an opportunity and ability to transition away from covered interconnection in the event their interconnection agreements or pathways must change due to national security. As the Commission is aware, negotiating interconnection agreements is complicated, and rerouting traffic patterns is not something that can happen

[19] *See, e.g.*, *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Second Report and Order and Second Further Notice of Proposed Rulemaking, ET Docket No. 21-232, FCC 25-71 (Oct. 19, 2025) ("*Second Report and Order*"); *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered Routers*, Public Notice, ET Docket No. 21-232, DA 26-286 (Mar. 23, 2026); *FCC's Public Safety Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List*, Public Notice, WC Docket No. 18-89 et al., DA 26-78 (Mar. 23, 2026); *AT&T Services, Inc. Petition for Expedited Waiver of Sections 2.932(b) and 2.1043(b) of the Commission's Rules to Permit Targeted Class I and Class II Permissive Hardware Changes to Covered Routers*, Order, ET Docket No. 21-232, DA 26-491 (May 15, 2026).

overnight. If the Commission is going to revoke domestic section 214 authorization for any entity, interconnected carriers must have ample opportunity to respond accordingly by finding new interconnection partners.

C. Any Rules or Prohibitions Must Apply Prospectively

Finally, the Commission should not apply any prohibition retroactively. This approach is consistent with Commission rules related to covered equipment and allows the Commission to "avoid the '[e]conomic harms associated with removing and replacing Covered List equipment."[20] Eliminating access to these already vital interconnection points will also likely deprive consumers of access to important communications, or increase the cost of receiving such communications, which will in turn require carriers who simply connect to these facilities to have to identify other facilities that purport to meet the Commission's requirements and without consumers losing needed service.

V. CONCLUSION

NTCA shares the Commission's goal of protecting the nation's communications infrastructure from threats to national security. Proposals in the *Notice*, however, that would prohibit telecommunications carriers from interconnecting with entities the Commission suggests in the *Notice* are a threat to national security would impact long-running IP interconnect proceedings. To avoid overbroad application and minimize harm, the Commission should narrowly focus prohibitions on entities named on the Covered List. Otherwise, any Commission action would impose an unrealistic and unachievable standard of knowledge on carriers. This tailored approach would also limit the burden of any action taken pursuant to this proceeding on

[20] *Second Report and Order* at ¶ 44.

carriers, especially small carriers, who are already working closely with the Commission and others to secure their networks.

Respectfully submitted,

By: /s/ Justin Faulb
Justin Faulb
Tamber Ray
Brian Ford
4121 Wilson Boulevard
Suite 1000
Arlington, VA 22203
703-351-2000 (Tel)

Dated: June 8, 2026