Before the
Federal Communications Commission
Washington, D.C. 20554

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

Comments of the
Telecommunications Industry Association

I. Introduction

The Telecommunications Industry Association ("TIA")[1] welcomes the opportunity to submit these comments in response to the Federal Communication Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking addressing national security risks in domestic telecommunications services.[2]

TIA is a U.S.-based trade association representing more than 400 trusted global manufacturers and vendors of telecommunications equipment. TIA members design, manufacture, and manage the world's digital infrastructure and information communications technology ("ITC") devices. TIA is also a standards-developing organization with a more than 80-year history of developing thousands of technical standards that encourage the secure and resilient deployment and operation of ICT equipment and networks. Our members make up the

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.

[2] Notice of Proposed Rulemaking, *Protecting Against National Security Threats in Domestic Telecommunications Service*, WC Doc No. 26-82 (Apr. 2026) ("NPRM").

trusted ICT global supply chain that impacts all segments of the global economy, and we share the Commission's goals of promoting trusted networks and encouraging network security.

TIA has a long-standing history of supporting the Commission's work to protect U.S. networks from foreign adversary suppliers deemed to pose a national security threat under the Secure and Trusted Communications Networks Act. TIA and its members work closely with government partners and across industry to build trusted communications infrastructure and protect the data that traverses it through our positions on various Federal Advisory committees, public-private partnerships, and collaboration with the U.S. government on promoting the use of trusted venders in delegations abroad. With respect to this proceeding, TIA supports the Commission's proposal to exclude specifically identified entities on the Covered List from receiving blanket Section 214 authority. At the same time, TIA urges the Commission to exercise caution before adopting broader measures, particularly restrictions on interconnection, that could unintentionally undermine network reliability, increase compliance burdens, and hinder U.S. technological leadership without materially mitigating national security concerns.

Interconnection, including with international networks and, in some cases, entities located in foreign adversary jurisdictions, fundamentally enables the connectivity necessary for Americans to participate in the global economy. As the United States pursues global leadership in strategic technologies like AI, and quantum computing, maintaining secure and reliable global communications infrastructure has never been more critical. Against this backdrop, overly broad restrictions on interconnection risk undermining these strategic objectives without meaningfully enhancing security.

Moreover, it has long been the policy of the United States to preserve international communications channels, including with foreign adversary countries, to ensure the continued flow of information for diplomatic, economic, and security purposes. We urge the Commission to act judiciously and enact targeted regulations that promote secure domestic networks while preventing unnecessary disruption to these longstanding principles and U.S. technological leadership abroad.

II. Entities Prohibited from Holding Blanket Section 214 Authority Should Be Limited to Specifically Enumerated Entities on the Covered List

TIA supports the FCC's proposal to exclude entities listed on the Covered List from receiving blanket Section 214 authority. Once an entity has been determined by national security experts to pose a threat to national security, it follows that the FCC has a vested interest in curtailing that entity's authority to operate in the country. Once an entity has been identified through established national security processes as posing a clear risk, restricting its ability to operate in U.S. telecommunications markets is both reasonable and consistent with the Commission's public interest obligations.

However, the Commission should clearly limit any such exclusion to **specifically identified entities**, rather than extending it to broad categories of equipment or undefined classes of actors. In recent months, the Administration has expanded entries on the FCC Covered List from specific enumerated entities to entire categories of products, often with little transparency into the specific determination that these decisions rely on. For example, the Commission has recently released Public Notices announcing broad exclusions of entire categories of devices

raise national security concerns if produced abroad.[3] These announcements marked a departure from passed Covered List updates, and TIA and our members have been working closely with the Commission to ensure the Administration's security concerns with foreign made IT equipment are addressed.

However, this evolving approach introduces significant uncertainty for industry stakeholders and risks sweeping in trusted entities, including U.S. companies and firms from allied nations, that operate within globally integrated supply chains. The ICT industry is inherently international, and many trusted entities maintain some level of global operational footprint. Without clear standards and transparency, categorical restrictions could inadvertently capture low-risk or trusted participants, undermining the Commission's objectives.

Accordingly, at this time TIA only supports the Commission prohibiting blanket 214 authority to specific enumerated entities on the Covered List as opposed to broad, categorical determinations that have been recently made. Any update to the domestic Section 214 rules should clarify that new restrictions *only* apply to specific named entities to ensure this prohibition is not abused by future administrations to achieve policy goals wholly unrelated to the security concerns that the Covered List is predicated upon. Limiting the scope in this manner will ensure that the Commission's actions remain targeted, proportionate, and aligned with the national security objectives underlying the Covered List framework.

[3] *See Protecting Against National Security Threats in Domestic Telecommunications Service,* Public Notice, DA 26-278 (2026); *see also Protecting Against National Security Threats in Domestic Telecommunications Service,* Public Notice, DA 25-1086 (2025).

III. Barring Interconnection Would Significantly Disrupt the ICTS Market and Undermine U.S. Technology Dominance

The NPRM seeks comment on national security concerns with allowing existing providers operating under domestic Section 214 authority to interconnect with Covered List entities or facilities that could contain equipment from the Covered List. While TIA appreciates the Commission's focus on mitigating potential vulnerabilities in network interconnection, prohibiting carriers from interconnecting with such facilities raises significant operational, economic, and policy concerns.

This is a far broader proposition than prohibiting the authority for entities demonstrated to pose a national security threat to operate in the U.S., especially at a time when the Administration is expanding its scope beyond specific named entities and adopting a categorical approach to additions to the Covered List as discussed above. Interconnection is foundational to modern telecommunications networks, enabling the exchange of traffic across interconnected systems domestically and globally. Prohibiting interconnection with facilities that are owned or operated by Covered List entities or those even those that have Covered List equipment would dramatically expand the Commission's regulatory authority. Such a requirement would effectively force Title II providers to effectively police the broader digital ecosystem, including third-party facilities, data centers, and any other upstream infrastructure, and could overburden ISPs and limit competition in the broader ecosystem. These providers would be forced to attest with certainty that interconnection with facilities that *could* contain Covered List is not occurring, something that is difficult to know for certain abroad or in contexts of indirect interconnection. These prohibitions could additionally negatively impact U.S. enterprises that need to interconnect with facilities abroad by adding additional compliance costs and regulatory

burdens that would not be replicated for non-U.S. firms interconnecting with global ICT networks.

The potential of these burdens on U.S. enterprises is particularly concerning given the current period of rapid growth in U.S. data infrastructure. The United States is experiencing a surge in investment in data centers and advanced computing facilities, driven in large part by demand for artificial intelligence and other next-generation technologies. Many of these facilities rely on globally sourced components that have already been authorized for use and operation in the United States under the Commission's existing equipment authorization regime. In practice, these proposals could function as a de facto "rip-and-replace" requirement, forcing operators to sever connections with certain facilities without providing the funding mechanisms that have accompanied prior efforts of that nature. Such a situation could disrupt ongoing infrastructure investment, potentially impacting the United States' leadership in emerging AI technologies, as well as negatively impact service continuity in cross-boarder communications, such as providers interconnecting with subsea cable networks or ICT networks on our border. Even more concerning, this proposal itself would establish a regulatory precedent for future Administrations to enact prescriptive regulations that would impact the entire connected ecosystem.

Further, legacy telecommunications interconnection has diminished significantly over the last five years, with IP-to-IP interconnection expanding.[4] Within this context, the Commission has been exploring possible updates to its interconnection framework, especially in light of its network modernization efforts.[5] As the environment shifts, the Commission should refrain from

[4] *See* FCC Voice Telephone Services, status as of June 30, 2025 (May 2026).
[5] *See* Advancing IP Interconnection; Accelerating Network Modernization NPRM (Oct. 2025).

taking action in regard on interconnection until there is a clear path forward. Considering the due diligence and compliance obligations these proposals would introduce to telecommunications service providers, especially if the Commission expands the requirement beyond specifically named entities, the obligation could introduce more costs than benefits, while impacting competitiveness and innovation. Further, any security benefit these additional burdens would impose would be further offset as potentially at-risk entities will still have other technological solutions available that would not fall under these rules for providing cloud-based and data center services.

Accordingly, the FCC should not proceed with proposals that would prohibit interconnection with facilities that have Covered List equipment as this could undermine service reliability, unnecessarily impose ex post facto restrictions, and stretch the FCC's authority in counterproductive ways. If the Commission nonetheless determines that action is necessary, they should take efforts to restrict the scope as much as possible to avoid disruption to ongoing infrastructure investment and mitigate the potential for overburdensome and prescriptive regulations from future administrations. Some of the burdens on trusted ICT entities can be alleviated by limiting restrictions to named entities only, ensuring compliance burdens lie completely with the untrusted entities, establishing a waiver process to protect international communications, and providing a sufficient transition period for any prohibitions that would avoid drastic impacts on essential communications services.

IV. Collaborative Partnership in Established National Security Risk Management Forums Can More Effectively Address These Risks

Rather than barring interconnection through this proceeding, the Commission and the broader Administration should consider more direct, collaborative approaches that incentivize

the deployment of trusted digital infrastructure while preserving the flexibility necessary to address evolving risks. The United States already maintains a wide range of tools and established forums to address national security concerns associated with foreign adversary access to communications infrastructure. These mechanisms are specifically designed to bring together government and industry stakeholders to identify threats, share information, and develop practical mitigation strategies. These processes have had longstanding industry support and proven more flexible than prescriptive regulatory requirements, particularly in the rapidly evolving and complex ICT industry.

Building on these existing capabilities, the Commission should prioritize policies that encourage the adoption of widely recognized, industry-led cybersecurity and supply chain risk management standards. These frameworks provide a scalable and forward-looking mechanism for ensuring that the expanding data center and communications ecosystem in the United States is built on a foundation of trusted suppliers. Supporting and updating established public efforts—such as those led by CISA, NIST, and other interagency initiatives—can strengthen baseline security across the ecosystem without imposing rigid constraints that may become outdated as technology evolves. Additionally, there are industry-led solutions that the Commission can leverage to ensure networks are built with trusted equipment and have proper supply chain and cyber risk mitigation in place. TIA's own SCS 9001 is one such standard and can add transparency to a network's supply chain and established risk management procedures.[6]

In addition, established public-private forums, for instance the Enduring Security Framework, the National Security Telecommunications Advisory Committee, Sector

[6] *See* TIA Release, SCS 9001 2.0 (available at https://tiaonline.org/resource/scs-9001-release-2-0-a-global-cybersecurity-and-supply-chain-security-standard-for-todays-evolving-threat-landscape/).

Coordinating Councils, and Information Sharing and Analysis Centers, all offer venues for stakeholders across the communications ecosystem to work collaboratively to address these risks. These bodies bring together telecommunications providers, equipment manufacturers, infrastructure operators, and government agencies, each of whom plays a distinct role in managing data security risks. Through these forums, participants can identify emerging threats, develop coordinated responses, and explore innovative technological solutions in a manner that reflects the operational realities of modern networks.

Finally, the Administration may wish to consider more targeted approaches that directly engage facilities and infrastructure operators. For example, incentives tied to federal procurement, streamlined permitting, or other policy mechanisms could encourage the transition toward trusted suppliers and technologies without imposing broad, system-wide prohibitions. Such approaches would better align incentives across the ecosystem while avoiding unintended consequences for network reliability and global connectivity. Taken together, these collaborative measures offer a more flexible, effective, and forward-looking approach to managing national security risks than the broad restrictions contemplated in this proceeding. By leveraging existing tools and partnerships, the Commission can advance its security objectives while preserving the resilience and openness that are fundamental to U.S. communications networks.

V. Conclusion

TIA appreciates the Commission's continued leadership in addressing national security risks in the telecommunications sector. TIA supports the Commission's targeted proposal to exclude specifically identified Covered List entities from receiving blanket Section 214 authority, as this approach appropriately addresses known risks while preserving the efficiency of existing regulatory frameworks.

At the same time, TIA urges the Commission to avoid adopting broader measures—particularly with respect to interconnection—that could have significant unintended consequences for network reliability, infrastructure investment, and U.S. technological leadership. By maintaining a targeted, transparent, and collaborative approach, the Commission can strengthen national security while preserving the innovation, resilience, and global competitiveness that define the U.S. communications ecosystem.

_/s/_____
Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard, Floor 9
Arlington, VA 22209

July 8, 2026