

Federal Communications Commission

Protecting Against National Security Threats in Domestic Telecommunications Service

47 CFR Part 63

[WC Docket No. 26-82; FCC 26-29; FR ID 345037]

AUTHORS

Jack Burnham

Senior Research Analyst, FDD's China Program

Washington, DC
July 7, 2026

Introduction

In the case of Covered List entities accessing domestic telecommunications infrastructure, the call is coming from inside the house.

While the Federal Communications Commission (FCC) has banned the use of federal funding for procuring equipment or services from foreign firms that pose a documented national security risk, the commission still allows these firms to automatically provide domestic telecommunications services under its blanket Section 214 authorization. This authorization, which was initially intended to lower barriers to entry and improve market efficiency by foregoing a case-by-case review of firms seeking to provide services, previously allowed Chinese state-owned firms to provide telecommunications services without the need for FCC approval.

However, the FCC can rectify this issue by closing the domestic Section 214 loophole. The Ninth Circuit's decision in *China Unicom (Ams.) Operations Ltd. v. FCC* gave the commission statutory authority to revoke domestic Section 214 authorizations, opening an avenue for further targeted enforcement efforts. Moreover, the commission's previous national security orders regarding submarine cables and the equipment authorization process offer firm legal grounding to treat Covered List entities as an entire class and, as such, curtail their access to certain authorizations based on their designated status.

The FCC should revoke blanket Section 214 authorization from Covered List entities while preventing domestic carriers from interconnecting with foreign providers linked to foreign adversaries.

Blanket Domestic Section 214 Authorization to Covered List Entities Is a National Security Risk

The blanket entry certification provided to domestic telecommunications providers under Section 214 was intended to provide a free and open market to build national networks without undue interference, allowing competition to flourish while retaining the commission's capacity to regulate abusive behavior.¹ This policy remains an inherent market efficiency within the United States — firms can acquire interstate networks with limited burdens to entry, lowering consumer prices by producing economies of scale.

However, this inherent openness also presents a key national security risk — once inside the U.S. domestic telecommunications market, the current structure of blanket domestic Section 214

¹ Communications Act of 1934, §214, ch. 652, 48 Stat. 1064, 1075.

authorization allows firms associated with foreign adversaries to purchase, maintain, and access interstate telecommunications infrastructure. This process previously allowed both state-owned firms, such as China Telecom, and other firms with ties to Beijing to openly operate in the United States under the same regulatory framework as domestic providers.² Along with gaining albeit limited market share given the predominance of American legacy carriers, this authorization allowed Chinese state-owned firms direct access into the heart of U.S. network infrastructure.

Nonetheless, shifting enforcement of domestic Section 214 authority has also allowed the commission to dismiss certain Covered List entities from American networks. In 2021, the commission revoked China Telecom Americas' (CTA's) domestic and international authorization after the firm had been placed on the Covered List, a move that the U.S. Court of Appeals for the DC Circuit effectively upheld in December 2022.³ The commission also revoked China Unicom Americas' (CUA's) domestic and international authorizations due to national security concerns, a move that was upheld by the Ninth Circuit Court in 2024.⁴ The revocations of voice authorization were later extended to providing internet services under the commission's net neutrality ruling in 2024, further removing these firms from the broader U.S. telecommunications sector, though this rule was blocked by the Sixth Circuit Court of Appeals in 2025.⁵

The FCC Can Target Covered List Entities as a Broader Class for Domestic Section 214 Revocation

The FCC's prior removal process has been predicated on targeting specific firms rather than treating entities on the Covered List as an entire class whose designation automatically endangers their domestic Section 214 authorization. While this model has been supported by the federal judiciary — the commission has consistently won its cases involving domestic Section 214 revocations — it also relies on evidence specific to each entity, leaving dangerous enforcement gaps despite previously demonstrated risks.

In the case of CUA, the FCC prevailed in court due to CUA's history of misrepresentation before the commission and Congress and its ties to Beijing.⁶ The CUA decision also offered a landmark affirmation of the commission's power to unilaterally revoke a Section 214 authorization using

² David DiMolfetta, "FCC proposes blocking high-risk firms from automatic telecom market approvals," *NextGov/FCW*, April 30, 2026. (<https://www.nextgov.com/policy/2026/04/fcc-proposes-blocking-high-risk-firms-automatic-telecom-market-approvals/413235>)

³ *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2022)

⁴ *China Unicom (Ams.) Operations Ltd. v. FCC*, 124 F.4th 1128 (9th Cir. 2024)

⁵ Safeguarding and Securing the Open Internet, Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, FCC 24-52, 39 FCC Rcd 4975 (2024); *Ohio Telecom Ass'n v. FCC*, 124 F.4th 993 (6th Cir. 2025)

⁶ *China Unicom (Ams.) Operations Ltd. v. FCC*, 124 F.4th 1128 (9th Cir. 2024)

its implied powers under the Communications Act of 1934, providing a stable legal footing for the FCC to act under its current statutory authority.⁷

The combination of the CUA decision and prior commission actions suggests that the FCC has both the statutory authority and the national security justification to unilaterally issue a blanket revocation for any entity on the Covered List. Since the CUA decision, the FCC has adopted a “presumptive disqualifying condition” for Covered List entities seeking to access certain segments of the U.S. telecommunications sector, setting a standard that can be adopted for other authorization programs.⁸ While this standard, which applies to applications for submarine cable licenses, is distinct from blanket domestic Section 214 authorization, it sets a precedent for treating Covered List entities as a class deserving strict regulatory scrutiny.⁹

Moreover, the FCC has used Covered List designations, in the absence of additional findings, as justification for license revocations and other penalties under its national security mandate. In November 2025, the commission modified its equipment authorization program to both prospectively and retrospectively revoke authorization for Covered List entities.¹⁰ The commission has also expanded its use of the Covered List, often with waiver exceptions to account for case-by-case submissions, to address other national security challenges, such as those posed by foreign-produced drones and routers.¹¹

Recommendations

To protect U.S. national security, the commission should prevent Covered List entities from accessing the U.S. telecommunications network by barring them from receiving automatic domestic Section 214 authorization. Moreover, the FCC should ensure that domestic carriers cannot interconnect with infrastructure or services owned and operated by Covered List entities,

⁷ Ibid.

⁸ Review of Submarine Cable Landing License Rules & Procedures to Assess Evolving Nat'l Security, Law Enft, Foreign Policy, & Trade Policy Risks, 90 Federal Register 48648, October 27, 2025.

⁹ Ibid.

¹⁰ Protecting Against Nat'l Security Threats to the Commc'ns Supply Chain Through the Equipment Authorization Program, 90 Federal Register 53227, November 25, 2025.; Jack Burnham and Annie Fixler, “Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program,” *Foundation for Defense of Democracies*, December 22, 2025. (<https://www.fdd.org/analysis/2025/12/22/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the-equipment-authorization-program-2>)

¹¹ Jack Burnham, “FCC Ban on Foreign-Produced Routers Targets Chinese Firms Tied to Cybersecurity Risks,” *Foundation for Defense of Democracies*, March 25, 2026. (<https://www.fdd.org/analysis/2026/03/25/fcc-ban-on-foreign-produced-routers-targets-chinese-firms-tied-to-cybersecurity-risks>); Jack Burnham, RADM (Ret.) Mark Montgomery, and Craig Singleton, “Unleashing American Drone Dominance,” *Foundation for Defense of Democracies*, May 1, 2026. (<https://www.fdd.org/analysis/2026/05/01/unleashing-american-drone-dominance>)

closing a potential backdoor allowing foreign adversaries access to American critical infrastructure.

- **The commission should exclude any entity identified on the Covered List from being authorized to provide interstate telecommunications services pursuant to blanket domestic Section 214 authority.** The FCC should close the loophole allowing Covered List entities blanket access to the domestic telecommunications sector even while posing a recognized national security risk. This ban should extend to Covered List entities barred from providing either equipment or services and block transfers of existing authorizations from domestic providers to listed providers. The commission should also begin the process of revoking preexisting domestic Section 214 authority using the framework outlined in the Foreign Adversary Control Report and Order.
- **The commission should require all entities “owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary” to apply to receive domestic Section 214 authority.** While the Covered List designates firms that have demonstrated a risk to U.S. national security, other telecommunications entities may pose a similar risk due to their fealty to Chinese national security law, which mandates their involvement in state-sponsored espionage. This risk has been previously defined by the commission in its Foreign Adversary Control Report and Order and its Submarine Cable Report and Order, both of which rely on the definition above to prevent malign foreign intrusion into U.S. networks.
- **The commission should require that any Covered Listed entity seeking approval for domestic Section 214 authority submit an individual application.** Should a Covered List entity seek domestic Section 214 authority to provide interstate telecommunications services, the commission should require it to issue a detailed request for consideration. This process should be similar to receiving international Section 214 authority, in which applications are referred to executive branch agencies, including Team Telecom and other national security agencies.
- **The commission should exclude any entity that installs covered equipment or services from blanket domestic section 214 authority.** The commission has previously highlighted the danger posed by covered equipment and services through a range of efforts, along with noting the danger of equipment produced and tested by foreign adversaries more broadly through its Bad Labs initiative and its listing of routers. As such, the commission should ensure that any entity that operates equipment or services from a Covered List entity cannot qualify for blanket Section 214 authority.

- **The commission should prohibit telecommunications carriers from interconnecting with entities barred from receiving domestic Section 214 authority.** Covered List entities should not be capable of indirectly gaining access to the U.S. network via interconnection with domestic carriers that maintain domestic Section 214 authority. These restrictions should extend to prohibit interconnection with any facilities, including points of presence and data centers, owned or operated by entities on the Covered List.

Conclusion

The commission should ensure that Covered List designation entails losing access to blanket Section 214 authorization, restricting firms that pose documented national security risks from freely accessing American networks without regulatory scrutiny. The cost of inaction — measured in both dollars and national security risk — grows every day.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the commission's ongoing policy work.