Federal Communications Commission

Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program

47 CFR Parts 1 and 2
[ET Docket No. 24-136; FCC 26-28; FR ID 345588]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Jiwon Ma
Senior Policy Analyst, FDD's Center on Cyber and Technology Innovation

Johanna Yang
Policy Analyst, FDD's Center on Cyber and Technology Innovation

Washington, DC
July 14, 2026

Introduction

The Federal Communications Commission's (FCC's) proposal to strengthen oversight of Telecommunications Certification Bodies (TCBs) and Measurement Facilities (test labs) is a necessary step toward addressing a longstanding gap in U.S. tech supply chain security.

The following outlines how China is manipulating and can exploit the FCC's equipment authorization process to harm U.S. national security. The comment also proposes a range of remedies to strengthen the integrity of the FCC process: prohibiting the recognition of testing facilities located in countries without a Mutual Recognition Agreement (MRA) or similar arrangement, proactively revoking previously issued accreditations, and expanding the definition of foreign ownership to include other mechanisms of control or influence.

Adversarial Control Over Test Labs Poses a Critical National Security Risk

Adversarial control over the certification process that governs the U.S. telecommunications technology ecosystem poses a systemic national security risk. TCBs and test labs are critical gatekeepers for thousands of telecommunications devices entering the U.S. market, including smartphones, routers, modems, and other equipment that transmits and receives voice, data, and video signals.[1] These entities handle highly sensitive proprietary data submitted by manufacturers — engineering documents, radiofrequency emissions, and other critical systems — and directly affect the types of hardware that can legally be imported into the United States.[2] Thus, if adversaries gain access to this layer of the supply chain, they can introduce vulnerabilities at scale, long before devices reach consumers or critical systems.

These risks cannot be divorced from China's pattern of behavior. Beijing aggressively blurs the lines between its nominally private technology sector and its military-industrial complex, with policies such as military-civil fusion mandating civilian firms to cooperate with defense contractors.[3] These efforts have only expanded as China has engaged in its unprecedented military buildup, forcing Chinese firms to divulge commercial secrets and collaborate on

[1] U.S. Federal Communications Commission, "Equipment Authorization – RF Device." (https://www.fcc.gov/oet/ea/rfdevice)
[2] RADM (Ret.) Mark Montgomery and Jiwon Ma, "Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program," *Foundation for Defense of Democracies,* April 14, 2025. (https://www.fdd.org/analysis/2025/04/14/promoting-the-integrity-and-security-of-telecommunications-certification-bodies-measurement-facilities-and-the-equipment-authorization-program)
[3] Jack Burnham and Johanna Yang, "Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control," *Foundation for Defense of Democracies*, July 21, 2025. (https://www.fdd.org/analysis/2025/07/21/protecting-our-communications-networks-by-promoting-transparency-regarding-foreign-adversary-control)

computing, communications, drones, and other technologies to fuel the modernization of the People's Liberation Army (PLA).[4]

This blurring is further obscured by China's national security laws, including its 2017 National Intelligence Law, which requires Chinese citizens and firms to cooperate with intelligence and security officials — regardless of where the citizen or firm is physically located.[5] This legal architecture raises significant concerns over the security of TCBs operating within Beijing's jurisdiction. Chinese law offers substantial leeway for authorities to influence TCBs and other facilities located within the PRC or its special administrative regions. Even U.S. and allied firms that operate in PRC territory or employ PRC-based personnel can be coerced.

Recommendations

The commission should strengthen the security of critical technology supply chains by prohibiting the recognition of adversarial test labs, revoking previous accreditations, and ensuring that foreign adversaries cannot circumvent its restrictions by expanding its definition of foreign ownership to include other mechanisms of control or influence.

- **The FCC should adopt rules that would prohibit the recognition of test labs, TCBs, or laboratory accreditation bodies that are in, or that conduct testing, certification, or accreditation in, countries that lack an MRA or trade agreements that provides for reciprocity with the United States.** The absence of an MRA limits reciprocal oversight, enforcement, and market access for U.S. testing facilities, particularly within China and Hong Kong. Excluding these jurisdictions from recognition will secure critical technology supply chains while strengthening domestic and allied demand for testing facilities.

- **The FCC should withdraw recognition of those test labs, TCBs, and laboratory accreditation bodies in countries that lack reciprocity with the United States and are already recognized.** While prohibiting the certification of new test facilities within non-MRA countries or non-Reciprocal Economies is critical, the commission must go further

[4] RADM (Ret.) Mark Montgomery and Jiwon Ma, "Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program," *Foundation for Defense of Democracies*, April 14, 2025. (https://www.fdd.org/analysis/2025/04/14/promoting-the-integrity-and-security-of-telecommunications-certification-bodies-measurement-facilities-and-the-equipment-authorization-program)
[5] Jiwon Ma and Jack Burnham, "Promoting the Integrity and Security of Telecommunications Certifications Bodies, Measurement Facilities, and the Equipment Authorization Program," *Foundation for Defense of Democracies*, August 15, 2025. (https://www.fdd.org/analysis/2025/08/15/promoting-the-integrity-and-security-of-telecommunications-certifications-bodies-measurement-facilities-and-the-equipment-authorization-program)

to prevent older facilities — which functionally present the same set of risks — from circumventing restrictions.

- **The FCC should prohibit any test lab, TCB, or laboratory accreditation body directly or indirectly owned by, controlled by, or subject to the jurisdiction or direction of a non-Reciprocal Economy.** Beijing's legal and operational reach ensures that it can influence the testing process even if operated outside of the country. As such, the commission should prohibit such facilities from its accreditation process.

Conclusion

Securing the FCC's equipment authorization process is a strategic investment in U.S. national security and economic resilience and remains critical to protecting U.S. critical infrastructure and military readiness.

Addressing jurisdictional loopholes within the authorization process will strengthen the testing capacity and reduce dependency on adversary-controlled facilities to ensure that short-term efficiencies are never gained at the expense of long-term strategic resilience.

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