PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

FEDERAL COMMUNICATIONS COMMISSION

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

ET Docket No. 24-136

AUTHORS

RADM (Ret.) Mark Montgomery
Senior Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Jiwon Ma
Senior Policy Analyst for the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Washington, DC
April 14, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

The Federal Communications Commission'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 the equipment authorization framework. As global supply chains become more complex and adversaries increasingly exploit technical processes to gain strategic advantage, the trustworthiness of the entities responsible for certifying telecommunications equipment must be treated as a matter of national security.

Adversary Access to the Certification Process is a Growing National Security Threat

The Commission's proposal recognizes a growing vector of systemic risk: adversarial control over the certification process that governs the U.S. telecommunications technology ecosystem. The 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] TCBs review engineering documents, test radiofrequency emissions, and determine whether these devices comply with FCC regulations. In doing so, TCBs and test labs handle highly sensitive, proprietary data submitted by manufacturers, conducting testing protocols and producing compliance certifications that the FCC relies on. Their judgments directly affect what hardware is legally imported into the United States for sale. Thus, if U.S. adversaries gain access to this layer of the supply chain, they can introduce vulnerabilities at scale, long before devices reach consumers or critical systems.

Assumptions of Trust No Longer Hold in Today's Threat Landscape

The TCBs and test labs under the direction or control of a foreign adversary pose a direct threat to U.S. national security. For decades, the integrity of this process was protected by a baseline assumption: that the entities performing these functions were impartial and operating in good faith. But that assumption no longer holds in today's threat landscape, particularly in the case of the People's Republic of China (PRC). Beijing maintains expansive authority over its domestic firms through a series of surveillance and intelligence laws, including its 2017 National Intelligence Law. Under this law, Chinese firms and individuals are legally required to assist with state intelligence operations,[2] effectively eliminating the legal distinction between corporates and the state.

The FCC has already acted in response to these risks. In 2024, the Commission appropriately denied the reauthorization of Huawei's Global Compliance and Testing Center due to these national security concerns.[3] However, Huawei is not the only Chinese-affiliated lab with a presence in the FCC's certification system. As noted in the FCC's fact sheet, other labs with ties

---

[1] U.S. Federal Communications Commission, "Equipment Authorization – RF Device." (https://www.fcc.gov/oet/ea/rfdevice)

[2] U.S. Department of Homeland Security, "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China," page 7. (https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf)

[3] U.S. Federal Communications Commission, "Global Compliance and Testing Center of Huawei Tec," April 22, 2024, page 1. (https://www.fcc.gov/sites/default/files/Global_Compliance-signed.pdf)

to Chinese state-owned enterprises, the People's Liberation Army, and even direct PRC government affiliations have collectively reviewed thousands of devices intended for the U.S. market.[4]

Moreover, the threat does not arise solely from ownership. Foreign adversary governments increasingly rely on corporate proxies — often appearing to be private companies — to advance state-directed strategic goals. Adversarial influence can be exerted through complex investment structures, joint ventures, or minority ownership stakes that fall below the FCC's existing 10 percent thresholds. Through shell companies, these entities can serve as a channel for circumventing existing FCC bans on covered equipment. The PRC routinely deploys such mechanisms to obfuscate state control and circumvent transparency. These structural realities render the FCC's Covered List framework[5] alone insufficient for identifying and disqualifying bad actors.

Technical Standards are Poor Substitutes for National Security Measures

Compounding this vulnerability is the fact that existing eligibility requirements for TCBs and test labs rely primarily on international technical standards like ISO/IEC 17025 and ISO/IEC 17065. These frameworks assess laboratory competence and impartiality, but they do not evaluate national security risks such as foreign government control or systemic susceptibility to espionage.[6] In today's threat environment, these omissions are no longer acceptable. Technical compliance does not guarantee trust. In practice, adversary-controlled labs may approve equipment embedded with malware or other vulnerabilities, falsify compliance reports, or steal proprietary information and market intelligence from U.S. companies for the benefit of their state. If changes are not made to the eligibility criteria for TCBs and test labs, these risks will undermine the credibility of the equipment authorization system and expose U.S. communications infrastructure to national security threats.

The Commission's proposed reduction in the ownership and control threshold from 10 to 5 percent is an important step in the right direction. However, the Commission must go further. Security risk is not measured by percentages alone — it is shaped by intent, influence, and legal subordination. A static list or ownership rule cannot keep pace with a dynamic threat.

Recommendations

To strengthen the integrity of the equipment authorization process, the Commission should adopt a more comprehensive risk-based approach to the eligibility of TCBs and test labs. The following recommendations are intended to mitigate foreign influence to ensure that only trusted, independent entities are authorized to certify equipment for the U.S. market.

---

[4] U.S. Federal Communications Commission, "Fact Sheet: FCC Voting This Week on Proposal to Ban "Bad Labs"," May 21, 2025, page 1. (https://docs.fcc.gov/public/attachments/DOC-402704A1.pdf)

[5] U.S. Federal Communications Commission, "List of Equipment and Services Covered By Section 2 of The Secure Networks Act." (https://www.fcc.gov/supplychain/coveredlist)

[6] ISO, "ISO/IEC 17025: Testing and calibration laboratories," (https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html); ISO, "ISO/IEC 17065:2012(en): Conformity assessment — Requirements for bodies certifying products, processes and services," (https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en)

1. **Expand disqualification criteria to include entities under the jurisdiction, direction, or control of foreign adversaries.**

The Commission should broaden its eligibility criteria for TCBs and test labs to reflect the full spectrum of risk posed by adversarial influence and control. Specifically, it should disqualify entities not only listed on the FCC's Covered List but also those subject to the jurisdiction, direction, or control of a foreign adversary, consistent with federal definitions under the Committee on Foreign Investment in the United States. This approach would enable the FCC to effectively assess geopolitical risk, even in cases where direct ownership is obscured.

2. **Adopt a rebuttal presumption of ineligibility for PRC-based or PRC-controlled entities.**

Given the PRC's current regulatory environment, including national security laws that coerce corporate cooperation with state intelligence objectives, firms operating under PRC jurisdiction cannot credibly demonstrate operational independence from the Chinese government. This presents a material compliance and reputational risk to U.S. markets. Therefore, all PRC-based or PRC-controlled entities must be assumed to be under state influence. The Commission should adopt a rebuttable presumption that any TCB or test lab based in or controlled by PRC-affiliated entities is ineligible for recognition. Firms seeking to participate in the FCC's equipment authorization process should carry the burden of proof in demonstrating both legal separation and independent governance, verified through transparent documentation and interagency review.

3. **Conduct periodic reassessment of recognized TCBs and test labs based on new intelligence, regulatory findings, or shifts in ownership/control.**

The current eligibility framework relies heavily on international technical standards, which do not evaluate national security posture or adversary-state exposure. The Commission should integrate a national security screening process into both the initial recognition and renewal stages for TCBs and test labs. This review should be modeled on existing FCC practices, such as those used in the IoT Cybersecurity Labeling Program,[7] and informed by interagency coordination. Doing so would ensure that technical competence is paired with operational trustworthiness.

4. **Empower the Office of Engineering and Technology to suspend or revoke recognition of high-risk entities.**

To ensure that the Commission can act swiftly in response to emerging threats, the FCC should codify the authority of the Office of Engineering and Technology to suspend or revoke recognition of TCBs and test labs suspected of presenting national security concerns. This authority should include the ability to take interim or emergency action where there is sufficient evidence to warrant further review, without requiring prior designation of the entity on a federal restricted list. Doing so will allow the Commission to proactively safeguard the integrity of its certification regime while maintaining procedural flexibility and alignment with interagency threat assessments.

[7] U.S. Federal Communications Commission, "U.S. Cyber Trust Mark." (https://www.fcc.gov/CyberTrustMark) U.S. Federal Communications Commission, "Fact Sheet: Cybersecurity Labeling for Internet of Things," February 22, 2024, page 1. (https://docs.fcc.gov/public/attachments/DOC-400674A1.pdf)

TCBs and test labs are not passive validators — they are entrusted with shaping the security posture of devices used throughout American homes, businesses, and critical infrastructures. This proceeding presents an opportunity to secure the foundation of the authorization system itself by ensuring that only trusted, independent, and accountable entities are empowered to validate the safety and compliance of devices entering the U.S. market.