Federal Communications Commission

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

Docket No. 24-136; FR ID 302403; CFR Part 2

AUTHORS

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

Jack Burnham
Research Analyst, FDD's China Program

Washington, DC
August 15, 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 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.

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 radio frequency emissions, and determine whether devices comply with FCC regulations — handling highly sensitive, proprietary data in the process. 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.

The decisive factor in determining eligibility for participation in the FCC's program should be whether an entity is subject to foreign influence, regardless of where the entity is geographically domiciled or what its ownership structure looks like.

The following outlines how the People's Republic of China (PRC) is manipulating and can exploit the FCC's equipment authorization process to harm U.S. national security and proposes a range of remedies to strengthen the integrity of the FCC process.

PRC Blurs Lines Between Civilian and Military Sectors to Gain Leverage Over U.S. Market

China aggressively blurs the lines between its nominally private technology sector and its military industrial complex, with policies such as military-civil fusion mandating that civilian firms cooperate with defense contractors. These efforts have only expanded as Beijing has engaged in its unprecedented military build-up, forcing Chinese firms to divulge commercial secrets and collaborate on computing, communications, drones, and other technologies to fuel the modernization of the People's Liberation Army (PLA).[2] 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 firm is physically located.[3]

---

[1] U.S. Federal Communications Commission, "Equipment Authorization – RF Device," accessed August 14, 2025. (https://www.fcc.gov/oet/ea/rfdevice)

[2] 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)

[3] 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)

This issue 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.

Chinese Firms' Role in Equipment Authorization Process Enhances Beijing's Market Power

China's role within TCBs and other laboratory testing reinforces its manufacturing dominance within the telecommunications sector, with approximately 75 percent of FCC-recognized testing for telecommunications and network equipment taking place in the PRC.[4] Proximity of manufacturing plants to these testing facilities allows companies to move prototypes directly from factory floor to a test lab within hours, shortening lead times and lowering costs. Over time, this co-location creates high switching costs and path dependency, locking companies into China-based production and certification. Chinese manufacturers benefit from economies of scale and scope from these hubs — sharing industrial infrastructure, specialized labor, and suppliers across multiple product types. This clustering effect cements China's position as the global center for electronics production and certification while allowing major firms to influence each aspect of the supply chain, from design to certification.[5]

Furthermore, such concentration means that if access to these hubs is blocked, both manufacturing output and certification capacity can be lost simultaneously. Because network effects magnify these dependencies — the more firms rely on these hubs, the higher the cost and difficulty of moving operations elsewhere — even a localized disruption would trigger cascading delays across global production schedules. In a crisis, U.S. companies — and even elements of the U.S. defense industrial base — could face shortages, production delays, and potential shutdowns.

Chinese firms have embraced uncompetitive practices — from consolidation to subsidies — to gain global market share in certified telecommunications and network equipment sold worldwide, including those entering the U.S. market. A combination of state subsidies, state-backed consolidation, and selective enforcement allows PRC-based labs to tilt the playing field.[6] Preferential treatment for Chinese firms — such as faster turnarounds, flexible review processes, or lax compliance enforcement — increases their speed-to-market advantage. Over time, this pressures foreign firms to co-locate production in China to gain comparable efficiencies, further reinforcing PRC dominance in both manufacturing and certification.

---

[4] David Shepardson, "US agency votes to bar Chinese labs deemed security risks from testing US electronics," *Reuters*, May 22, 2025. (https://www.reuters.com/business/media-telecom/us-agency-votes-bar-chinese-labs-deemed-security-risks-testing-us-electronics-2025-05-22)

[5] Chenxi Jin, Chenjing Fan, Yiwen Gong, Xinran Huang, Shiqi Li, Runhan Liu, Chunwei Guo, and Yuxin Liu, "An analysis of spatial changes in the manufacturing industry in China's three major urban clusters from 2015 to 2019 using POI data," *Nature*, March 3, 2025. (https://www.nature.com/articles/s41598-025-90373-w)

[6] 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)

Balancing National Security and Market Accessibility in Test Lab Re-Shoring

In the event of a military crisis in the Indo-Pacific, disruptions would not only halt manufacturing but also cut off access to PRC-based test labs relied upon for FCC certification. Losing both production and certification channels would multiply the impact of any supply shock, forcing American firms and the U.S. defense industrial base to ration key components or halt production altogether. This could delay deployment of critical systems and reduce interoperability with allies and partners.

Reliance on PRC-based labs risks exposing sensitive proprietary and technical data to adversary intelligence collection and increases the likelihood of supply chain compromise and data exfiltration. These vulnerabilities can undermine U.S. power projection when it is needed most. What may appear as a marginal cost advantage today is not a true cost-for-cost comparison. It is an exchange of short-term savings for long-term strategic failure. The potential downside includes degradation of U.S. warfighting capabilities and erosion of competitiveness in high-value markets, dwarfing any immediate financial gains.

These trends argue for the gradual re-shoring of TCBs and other test labs within the United States and its closest allies and partners. In the short term, this shift will raise certification costs and create temporary backlogs while new capacity ramps up. There is a risk that companies will pass on these costs to consumers. However, in competitive sectors like smartphones, routers, and IoT devices, buyers are highly price-sensitive, making it risky for manufacturers to pass on small per-unit price increases.[7]

Cost absorption will vary by size of the firms. Large firms producing at scale can typically absorb certification costs, since they amount to only a fraction of a high-volume product's price. These manufacturers already manage volatile costs from fuel, raw materials, and tariffs the same way — preferring to protect their customer base instead of raising prices for marginal gains.[8] In contrast, smaller firms, which often produce in low volumes, face proportionally higher certification costs, which make up a much larger share of the total product cost. This makes these costs harder to absorb without eroding margins, pricing products out of the market, or passing the cost to consumers. Supporting smaller firms through targeted incentives can reduce the impact of these effects, ensuring that both large and small producers benefit from a more secure and resilient system.

Ensuring affordable certification in the market reinforces the importance of diversifying and re-shoring test lab capacity across trusted locations. Doing so reduces the risk of disruption, keeps certification affordable and accessible for all producers, and creates redundancies critical to national security and long-term economic resilience.

---

[7] Henry B. Weil, "Competitive Dynamics — Winning in Technology Markets," *MIT Sloan School of Management*, November 15, 2023. (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4632772)
[8] Jeffrey A. Sonnenfeld, Laura D. Tyson, and Stephen Henriques, "Big Companies Are Not the Inflation Villain," *Fortune*, September 30, 2024. (https://fortune.com/2024/09/30/kamala-harris-economic-message-price-gouging-inflation-politics/?abc123)

Recommendations

To strengthen the integrity of the equipment authorization process, the Commission should adopt a comprehensive, risk-based approach that weighs both the national security risks and the economic impact of relying on entities with ties to foreign adversarial nations. 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 while minimizing market disruptions and maintaining accessibility to certification services.

- **The Commission should extend the prohibitions in the current rule for TCBs, test labs, and laboratory accreditation bodies to include those facilities subject to the influence of a foreign adversary, regardless of physical location or nominal corporate structure**. Chinese law and regulations, such as the National Intelligence Law and Data Security Law, offer Beijing extensive authority to force cooperation from companies and individuals under its jurisdiction, including those operating outside the mainland. Because Beijing can exert control through legal mandates, corporate governance structures, and employee placement, changing the physical location of a test lab is insufficient to mitigate risk posed by the PRC. As a possible alternative to wholesale prohibitions, the Commission could establish a rebuttable presumption of ineligibility for such entities, coupled with strict requirements that none of their employees, contractors, or subcontractors with access to sensitive information be located in adversarial states.

- **The Commission should prohibit test labs located in China or operated by PRC-headquartered entities from participating in the equipment authorization program.** China's role in the equipment authorization program not only enhances its firms' global competitiveness but also creates leverage points that could be exploited in a geopolitical crisis. Control over a key compliance gateway, like the FCC's equipment authorization programs, allows Beijing to indirectly shape market access, set de facto timelines, and subtly influence technical outcomes in ways that favor its domestic firms. Over time, this regulatory foothold compounds China's strategic advantage, making it harder for U.S. and allied manufacturers to diversify away from PRC-based manufacturing ecosystems.

- **The Commission should apply the framework outlined in Executive Order 13959 when assessing the national security threat posed by test labs and accreditation bodies located in foreign adversary nations**. EO 13959 directs agencies to evaluate supply chain risks by considering the broader legal, political, and security environment in which an entity conducts its business — in addition to its ownership structure and equity control.[9] This provides the Commission a clear executive and legal basis to weigh jurisdictional coercion, indirect influence, and historical patterns of behavior when determining whether an entity poses an unacceptable risk to the United States. Participation in FCC-recognized testing by PRC-based entities carries inherent risk,

[9] "Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies," 85 Federal Register 73185, November 12, 2020. (https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies)

regardless of whether that testing activity appears commercial in nature. Through EO 13959's framework, the Commission could conclude that PRC-based test labs present security risks simply by virtue of being subject to Chinese national security laws.

- **The Commission should rely on the definition of "controlled by a foreign adversary" set out in 15 U.S. Code § 9901**. This definition, which considers jurisdiction as a key factor, has been upheld in recent Supreme Court jurisprudence. The definition adequately captures adversaries' use of indirect control and coercive measures, such as minority shareholding or corporate governance structure, in exercising control over firms. Additionally, given China's use of these complex corporate structures and ownership arrangements, the Commission should consider lowering the ownership threshold for determining "control" from 20 percent to 5 percent and consider firms' historical patterns of behavior for regulatory determinations.

- **The Commission should formally incorporate the Office of Foreign Asset Control's Specially Designated Nationals and Blocked Persons List (SDN List) into the definition of "prohibited entities" for the TCB and test lab program.** The SDN List is public and well-maintained, and has strong private sector compliance mechanisms. By explicitly referencing the SDN List, the Commission would align its rule with existing federal laws and strengthen the federal law enforcement efforts to prevent foreign adversaries from influencing the lab test program without creating new administrative burdens.

- **The Commission should implement a range of policies to encourage both manufacturers and service providers to use U.S., allied, and partner-nation TCBs, test labs, and accreditation bodies**. The Commission should fast-track recognition for U.S.-based test laboratories and those located within trusted allies and partners, such as Japan, South Korea, Taiwan, and the European Union. The Commission should also consider reducing accreditation fees, offer targeted tax incentives, and launch a public-private partnership program to expand lab capacity in strategic locations. By lowering entry barriers and reducing fixed costs for new entrants, these measures would improve competition and quickly scale domestic and allied testing capacity while diluting China's current clustering advantage.

  In parallel, the Commission should provide incentives for manufacturers as well — such as expedited equipment authorization processing, reduced filing fees, or eligibility for grants — for companies that choose testing facilities in the United States and allied or partner nations. Tailoring these incentives to small and mid-sized firms would help offset costs associated with re-shoring, making it operationally and financially feasible to shift testing out of the PRC. Expanding domestic and allied testing capacity also creates economic spillovers — such as keeping high-value technical jobs in the United States, stimulating regional manufacturing ecosystems, and improving supply chain resilience — while avoiding significant cost shocks to industry by enabling gradual, market-driven diversification away from PRC-based facilities.

- **The Commission should strengthen post-market surveillance by requiring TCBs to engage independent reviewers or auditors rather than self-monitor their certification processes**. The current self-policing model intrinsically creates conflicts of interest, reduces accountability, and erodes market trust over time. Rather, an independent review introduces the same kind of checks and balances used in high-integrity financial auditing — ensuring that certification is not only technically sound but also impartial. A randomized assignment system in which TCBs review the work of other TCBs — combined with transparency requirements — would create a "mutual accountability loop" that deters collusion or retaliation while raising the overall standard of performance. By treating certification integrity as a market differentiator, the Commission would incentivize TCBs to compete on quality and trust, rather than just speed and cost. The Commission should ensure these reviewers have no financial ties to foreign-owned TCBs and must fall under the jurisdiction of the United States or its trusted allies and partners.

- **The Commission should regulate the relationship between TCBs and test labs to prevent vertical integration or undue influence**. Foreign adversaries, particularly China, have historically encouraged vertical integration in high-value sectors to capture market share, control critical supply chain choke points, and embed strategic dependencies. When the same entity controls both testing and certification, it concentrates decision-making power, reduces competitive pressure, and could create opportunities for regulatory capture. To counter this, the Commission should adopt a tiered restriction framework — ranging from complete bans on shared ownership to targeted, risk-based restrictions and enhanced disclosure requirements on corporate structure and subcontracting to better regulate entities with intertwined operations. This approach would preserve market competition, strengthen supply chain resilience, and close loopholes adversaries can exploit.

Conclusion

Securing the FCC's equipment authorization process is not just a regulatory exercise — it is a strategic investment in U.S. national security and economic resilience. Addressing these jurisdictional loopholes can strengthen the testing capacity and reduce dependency on adversary-controlled facilities. By doing so, the Commission can ensure that short-term efficiencies are never gained at the expense of long-term strategic resilience — protecting U.S. critical infrastructure and military readiness.