Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: ET Docket No. 24-136, Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program (Second Further Notice of Proposed Rulemaking)

Dear Secretary Dortch:

I write in support of the proposals set out at paragraphs 68 through 75 of the Second Further Notice of Proposed Rulemaking, FCC 26-28,[1] and respectfully urge the Federal Communications Commission (FCC) to adopt rules that would ultimately cease recognition, in phased stages, of test labs, Telecommunications Certification Bodies (TCBs), and laboratory accreditation bodies that are located in, or conduct their work in, countries that lack a mutual recognition agreement or comparable reciprocal trade agreement with the United States.[2]

This comment addresses three points: (1) the FCC's statutory authority to adopt a jurisdiction-based eligibility rule; (2) the reasoned basis for shifting from ownership screening to jurisdiction screening; and (3) the rule's economic effects, including its protection of American intellectual property and its support for domestic testing capacity.

Statutory authority. The FCC's authority to condition recognition of TCBs and test labs on national-security grounds is well established. Section 302(e) authorizes the FCC, when delegating certification and testing responsibilities to private entities, to "establish such qualifications and standards as it deems appropriate."[3] Section 302 more broadly permits reasonable regulations governing radiofrequency equipment consistent with the public interest, and Section 303(e) authorizes the xFCC to regulate the kind of apparatus used with respect to its external effects.[4] As the FCC recognized in the EA Security Report and Order, these provisions

[1] *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Second Report and Order, Order on Reconsideration, and Second Further Notice of Proposed Rulemaking, FCC 26-28 (rel. May 1, 2026), https://docs.fcc.gov/public/attachments/FCC-26-28A1.pdf [hereinafter Second FNPRM].

[2] I recognize that the comment period recently closed and submit this comment in reliance on the Commission's practice of accepting late-filed comments when doing so aids the record.

[3] 47 U.S.C. § 302a(e)(3); *see Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Notice of Proposed Rulemaking, FCC 24-58, ¶ 39 (rel. May 24, 2024), https://docs.fcc.gov/public/attachments/FCC-24-58A1.pdf [hereinafter NPRM].

[4] 47 U.S.C. § 303(e); *see* NPRM, *supra* note 2, ¶ 19.

provide authority to address national security concerns in administering the equipment authorization program, a point reinforced by the Secure and Trusted Communications Networks Act and the Secure Equipment Act of 2021.[5] A rule keyed to the legal jurisdiction in which testing and certification occur falls squarely within the "qualifications and standards" the FCC may set under Section 302(e), because the enforceability of the FCC's own inquiries against a lab is a direct measure of that lab's competence and reliability.

Reasoned basis. The record supports a determination that ownership-based screening alone is insufficient. The national security legal regime of the People's Republic of China (PRC) imposes obligations based on jurisdiction and legal presence, rather than merely on ownership or formal corporate control. Under the PRC National Intelligence Law (NIL), as amended in 2018, entities and individuals within the jurisdiction of the PRC are obligated to "support, assist, and cooperate" with state intelligence work.[6] These obligations are reinforced by the PRC National Security Law, which imposes upon enterprises, institutions, and other social organizations the responsibility and obligations to safeguard national security,[7] and the PRC Data Security Law, which expressly requires relevant organizations and individuals to cooperate when public-security or state-security organs obtain data for national security or criminal investigation purposes.[8]

Congressional testimony before the Senate Committee on Homeland Security and Governmental Affairs documents that these authorities reach Chinese entities and even the subsidiaries of U.S. companies operating under PRC jurisdiction.[9] The Department of Homeland Security's *Data Security Business Advisory* similarly warns that PRC legal authorities compel data sharing with

---

[5]NPRM, *supra* note 2, ¶ 19 (noting the Commission's broad statutory authority, predating the Secure Networks Act and the Secure Equipment Act, under sections 302 and 303(e) of the Communications Act and other statutory provisions, to take national security concerns into account when promoting the public interest).

[6]National Intelligence Law of the People's Republic of China (2017, as amended 2018), art. 7 ("All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law."), translation available at https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

[7] *National Security Law of the People's Republic of China* (2015), arts. 11, 13 (providing that PRC citizens, state bodies, enterprises, institutions, and other social organizations have the responsibility and obligation to safeguard national security, and providing for legal liability for failure to fulfill national-security obligations).

[8] *Data Security Law of the People's Republic of China* (2021), arts. 35–36. Article 35 requires relevant organizations and individuals to cooperate when public-security or state-security organs obtain data for national-security or criminal-investigation purposes; Article 36 prohibits organizations and individuals within the PRC from providing PRC-stored data to foreign judicial or law-enforcement authorities without approval of competent PRC authorities. The 2023 revised Counter-Espionage Law supplies still another statutory layer. Article 8 requires *all citizens and organizations* to support and assist counter-espionage work. Counter-Espionage Law of the People's Republic of China, as revised Apr. 26, 2023, effective July 1, 2023, art. 8, translated in U.S. Dep't of Defense, China Aerospace Studies Institute, *In Their Own Words* series (2023), available through https://www.govinfo.gov/app/details/GOVPUB-D301-PURL-gpo214863.

[9]*China's New National Security Laws: Risks to American Companies and Conflicts of Interest*: Testimony Before the S. Comm. on Homeland Security & Governmental Affairs (Sept. 24, 2024) (testimony of Rush Doshi), https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Doshi-2024-09-24.pdf.

the state.[10] Because these obligations attach by virtue of jurisdiction rather than ownership, a lab located in the PRC cannot, absent extraordinary circumstances, credibly demonstrate the degree of operational independence from governmental direction or compulsion contemplated by the impartiality requirement of ISO/IEC 17025 and ISO/IEC 17065, regardless of its formal ownership structure.[11] By the same reasoning, formal separation through a subsidiary structure does not eliminate the concern: where a subsidiary or other affiliate is subject to PRC jurisdiction, its legal obligations to comply with PRC national-security, intelligence, and data-access authorities remain notwithstanding the nationality or ownership structure of its parent corporation.

The FCC's enforcement experience confirms the point. The FCC has already withdrawn recognition from labs found to be owned or controlled by the PRC government, including a group of fifteen China-controlled labs.[12] These actions illustrate the core defect the proposed rule addresses: where a lab operates outside the reach of enforceable U.S. or reciprocal-agreement jurisdiction, its certifications cannot be reliably tested or corrected, and unreliable certifications flow into the domestic supply chain. Screening by ownership requires the FCC to trace and continually re-verify control relationships that adversary entities have every incentive to obscure. Screening by jurisdiction, by contrast, turns on the legal regime that governs the lab, which is stable, verifiable, and directly relevant to enforceability.

Economic effects and intellectual property. Test labs obtain pre-market access to American hardware, firmware, and design information.[13] The record notes how rapidly PRC competitors replicated a novel unlock technology after its commercial release; the risk is greater still for equipment on the Pre-Approval Guidance list, where labs handle sensitive, not-yet-marketed technologies.[14] Directing this work to labs subject to U.S. law or reciprocal-agreement obligations reduces the exposure of American innovators to misappropriation while ensuring that the FCC can compel timely responses to its inquiries, an enforcement capacity it lacks against

---

[10] U.S. Department of Homeland Security, *Data Security Business Advisory* (Dec. 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[11] *See* 47 C.F.R. § 2.948(a), (e) (requiring accreditation of test labs to ISO/IEC 17025); NPRM, *supra* note 2, ¶¶ 6, 12 (TCBs must meet ISO/IEC 17065 requirements, including carrying out their responsibilities in a "competent, consistent, and impartial manner").

[12] FCC, *FCC Denies Second Batch of 'Bad Labs' Controlled by China* (press release, Sept. 26, 2025), https://docs.fcc.gov/public/attachments/DOC-414863A1.pdf; *see also* Second FNPRM, *supra* note 1, ¶ 40 n.75 (noting that since September 8, 2025, the Commission has removed over 16 test labs that were an arm of, or owned by, the PRC government).

[13] Second FNPRM, *supra* note 1, ¶ 27 ("Test labs have privileged and early access to confidential information about new products given their role in the supply chain.").

[14] *Id.* ¶ 27 & n.53 (citing Patrick McGee, *Apple in China: The Capture of the World's Greatest Company* 341 (2025)) (noting reports that Huawei, Oppo, and Vivo devices mimicked Apple's Face ID unlock technology shortly after the iPhone X's release); *see also id.* ¶ 42.

actors that have used the Hague Service Convention to evade accountability.[15] Channeling testing toward jurisdictions where the FCC's process is enforceable reduces the risk that domestic firms lose proprietary technology as a condition of market access.

The transition burden appears to be manageable. In 2024, over 16% of devices receiving FCC IDs were already tested by labs in the United States or MRA economies,[16] and the FCC's fast-track Pre-Approval Guidance process further incentivizes migration to Trusted Test Labs.[17] A phased implementation, tied to renewal cycles, would allow capacity to expand in step with the transition.[18]

Suggested refinement. I encourage the FCC to adopt a definite implementation schedule rather than leaving the phase-out open-ended, so that industry can plan capacity investments with certainty. If the FCC adopts an interim fee for applications tested in non-reciprocal jurisdictions, I suggest it publish the fee schedule in advance and earmark the proceeds for enhanced post-market surveillance and for training the domestic testing workforce, so that the interim measure directly builds the capacity the final rule presumes.[19]

For these reasons, I respectfully urge the Federal Communications Commission to adopt the jurisdiction-based eligibility rule described in paragraphs 68 through 75 of the Second Further Notice.

Respectfully submitted,

Piero Tozzi
1455 Pennsylvania Ave NW
STE 225
Washington, D.C. 20004
America First Policy Institute

[15] *Id.* ¶ 29 (noting that "foreign actors from non-Reciprocal Economies have abused the protections of the Hague Service Convention to evade accountability for repeated violations" in the equipment authorization program).

[16] *Id.* ¶ 26 (citing Sporton Comments at 3) (in 2024, 3.6% of devices receiving FCC IDs were tested by labs in the United States and 12.5% by labs in MRA countries).

[17] *Id.* ¶¶ 20, 26, 31.

[18] *Id.* ¶ 71 (seeking comment on phasing out non-Reciprocal Economy test labs, TCBs, and laboratory accreditation bodies as they come up for renewed recognition, rather than withdrawing recognition from all labs on a certain date).

[19] *Id.* ¶ 72 (seeking comment on an additional fee for equipment tested in non-Reciprocal Economy test labs and on earmarking those funds for enhanced post-market surveillance or auditing and for training a domestic testing workforce).