The Heritage Foundation
214 Massachusetts Ave NE
Washington, DC 20002

September 3, 2024

The Honorable Jessica Rosenworcel
Chairwoman
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program, ET Docket No. 24-136, FR ID 228432.

Dear Chairwoman Rosenworcel,

The Heritage Foundation respectfully submits a comment for the proposed rulemaking, Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program. The proposed rule would prohibit telecommunications certification bodies (TCBs) and measurement facilities (test labs) directly or indirectly owned or controlled by an entity on the Covered List from participating in the FCC's equipment authorization program due to the risks these entities present to U.S. national security. The list includes telecommunications, video surveillance, cybersecurity, and anti-virus software equipment and services manufactured by 12 entities in China and Russia.[1] The Heritage Foundation supports this proposal and urges the Commission to consult other Executive Agencies that maintain lists of entities that present national security risks and to extend its prohibition to all entities owned or controlled by a foreign adversary.[2]

The FCC established the equipment authorization program in order to fulfill its statutory requirement to govern the interference potential of devices that emit radio frequency.[3] Through this program, the agency examines telecommunications equipment for harmful interference to radio communications and requires emissions to remain under certain levels. The FCC must approve and authorize any equipment before it can be marketed in or imported to the United States. In 2022, the FCC completed around 40,000 equipment authorizations.[4]

---

[1] Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, AO Kaspersky Lab, China Mobile International USA Inc., China Telecom Corp., Pacific Networks Corp, ComNet LLC, China Unicom Operations Limited, and Kaspersky Lab, Inc. FCC, List of Equipment and Services Covered By Section 2 of The Secure Networks Act, Last updated July 23, 2024. https://www.fcc.gov/supplychain/coveredlist (accessed August 27,2024)

[2] The People's Republic of China, including the Hong Kong Special Administrative Region; Republic of Cuba, Democratic People's Republic of Korea, Russian Federation, and Venezuelan politician Nicolás Maduro, 15 CFR § 7.4.

[3] 47 U.S.C. § 302

[4] Dusmantha Tennakoon, "TCB Surveillance," October 25, 2023, p. 3, https://www.fcc.gov/sites/default/files/53-TCB-Market-Surveillance-TCB_Oct_2023.pdf (accessed August 26, 2024).

The FCC does not currently recognize any test lab accrediting bodies or TCBs in China, Russia, or any other foreign adversaries. There are, however, at least 170 test labs in China out of over 600 labs recognized by the FCC worldwide. None of these labs appear to be directly owned by an entity on the Covered List, but we are uncertain if they are indirectly owned or affiliated with entities on the list.[5] The proposed rule will have a greater impact if the FCC extends the prohibition to other known threats from foreign adversaries. Of course, the FCC will need to determine how the remaining labs could then effectively meet the demand created by eliminating labs compromised by links to the Chinese Communist Party.

Extending the prohibition to entities owned or controlled by a foreign adversary is not new. In November 2019, the FCC issued a rule that prohibited Universal Service Fund recipients from using funds to procure Huawei and ZTE equipment after reports illuminated the national security risks these companies presented to U.S. communications infrastructure. Twenty-five percent of the Rural Wireless Association used Huawei or ZTE equipment at that time.[6] President Trump signed the Secure and Trusted Communications Networks Act into law in March 2020 and cemented the FCC's rule by prohibiting recipients of federal funds from procuring telecommunications equipment and services from a company that poses a national security risk to U.S. communications networks. The law also required the FCC to publish and maintain a list of such equipment or services, known as the Covered List, and established the Secure and Trusted Communications Networks Reimbursement Program to provide financial assistance to communications providers to rip and replace Huawei and ZTE equipment. To date, the FCC has approved $4.98 billion in reimbursement costs for communications providers.[7]

As part of implementing the Secure and Trusted Communications Networks Act, the FCC issued a final rule in February 2023 that banned authorizing communications equipment produced by entities on the Covered List. Additionally, in March 2024, the FCC adopted the Cybersecurity Internet of Things Labeling Report and Order that prohibited products owned, controlled, or affiliated with foreign adversaries from receiving the Cyber Trust Mark. This year, President Biden signed legislation that forces TikTok to divest from its Chinese-parent company ByteDance.[8] The Chinese Communist Party is a persistent threat to U.S. national security through its pervasive digital surveillance, intellectual property theft, corporate espionage, force tech transfer, cyber-hacking operations, and potential interference in critical telecommunications services. Furthermore, extending the prohibition would eliminate any labs using forced labor or

---

[5] In a search of the list of accreditation bodies, TCBs, and test labs found on the FCC's website, 174 test labs in China out of 652 labs were found. https://apps.fcc.gov/oetcf/eas/reports/TestFirmSearch.cfm (accessed on August 26, 2024). None of the test labs identify an entity on the Covered List as the lab's firm name.
However, the FCC's proposed rule cites 170 labs in China as of March 26, 2024 and 639 total FCC-recognized test labs. See footnotes 49 and 51 on p. 9. https://docs.fcc.gov/public/attachments/FCC-24-58A1.pdf.

[6] William Yuen Yee, "With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?," *CSIS*, December 10, 2020, https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn (accessed August 26, 2024).

[7] Jon Brodkin, "Telcos keep using "insecure" Chinese gear because of congressional inaction," *Ars Technica*, May 6, 2024, https://arstechnica.com/tech-policy/2024/05/us-plan-to-purge-huawei-from-telecom-networks-stalled-by-funding-shortfall/#:~:text=A%20few%20months%20later%2C%20Congress%20approved%20the%20Secure,The%20approved%20reimbursements%20total%20%244.98%20billion%2C%20Rosenworcel%20wrote (accessed August 26, 2024).

[8] Public Law No: 118-50.

committing other human rights abuses such as in the Xinjiang region. This action would be consistent with U.S. law. Congress prohibited the importation of goods made with forced labor in the Xinjiang region in the Uyghur Forced Labor Prevention Act.[9] Rather than eliminating the threat piecemeal through the Covered List, extending restrictions to foreign adversaries would eliminate the common denominator China presents.

The Heritage Foundation has maintained concerns over China's surveillance and influence over Americans through TikTok and other espionage and data-collection tools. A March 2023 report details how China's 2017 National Intelligence Law requires "any organization or citizen shall support, assist, and cooperate with state intelligence work according to the law."[10] In other words, any Chinese "private" entity can be reasonably presumed to be linked to the Chinese Communist Party.

The Commission seeks comment on the extent to which it "should impose eligibility restrictions for TCBs and test labs based on lists developed by Executive Branch agencies that reflect expert determinations about entities that pose national security risks."[11] Given the limited scope of the Covered List, it would be prudent for the Commission to consult other agencies that maintain lists of known entities that present national security risks to the U.S., such as the Department of Commerce's Entity List.

The FCC proposes requiring TCBs and test labs to report their direct or indirect equity and/or voting interest of 5% or more by any entity, down from the current 10% reporting threshold. The Commission states that it agrees with Executive Branch determinations that "instances less-than-ten percent foreign ownership interest – or a collection of such interests – may pose a national security or law enforcement risk." We ask that the agency explain in detail why entities with less than 10% pose a risk, but entities below 5% do not. The Commission should consider whether any level of ownership by an entity on the Covered List needs to be disclosed.

The Commission requests comment on how frequently TCBs or test labs should report ownership disclosures to the agency. Reporting requirements should be limited in effort to reduce an entity's paperwork burden, as required by the Paperwork Reduction Act, and paired with other reporting requirements if possible. For example, the Securities and Exchange Commission requires quarterly and annual earnings reports from publicly traded companies. Reporting requirements should be robust enough to ensure transparency, mitigate risk, and eliminate threats. While accreditation bodies perform full assessments of TCBs every two years, which may be sufficient for evaluating a lab's procedures, accuracy, effectiveness, and impartiality, this is too lengthy for change in ownership disclosures.

---

[9] Public Law No: 117-78.
[10] Kara Frederick, "TikTok Generation: A CCP Official in Every Pocket," Heritage Foundation *Backgrounder* No. 3757, March 22, 2023, p. 2 https://www.heritage.org/sites/default/files/2023-03/BG3757.pdf.
[11] 89 FR 55530, III. Discussion, para. 22, https://www.federalregister.gov/documents/2024/07/05/2024-14491/promoting-the-integrity-and-security-of-telecommunications-certification-bodies-measurement (accessed August 26, 2024).

In conclusion, the proposed regulation, if extended to include all entities owned and controlled by foreign adversaries, would greatly reduce the risk the Chinese Communist Party and other adversaries present to our critical telecommunications network, equipment, and services. Additionally, extending restrictions to entities on threat lists housed by other Executive Agencies would aid and bolster the FCC's efforts to address threats. The FCC will need to weigh the impact to the equipment authorization pipeline if all test labs from China are withdrawn from the program and establish a plan for meeting heightened demand. Lastly, the Commission needs to carefully determine the percentage of ownership that constitutes a threat to national security and the subsequent disclosure requirements.

Respectfully,
The Heritage Foundation

by:

/s/ Annie Chestnut

Annie Chestnut
Policy Analyst, Tech Policy Center