OFFICE OF COMMISSIONER BRENDAN CARR

FACT SHEET: FCC Voting This Week on Proposal to Ban "Bad Labs"

FCC Proposing to Prohibit Untrustworthy Actors, Including Those Tied to the CCP, From Reviewing or Approving Equipment for Use in the U.S.

WASHINGTON, DC, May 21, 2024—On Thursday, at the FCC's May Open Meeting, the FCC will vote on a proposal that would further strengthen the security of America's communications networks. Under the bipartisan proposal, which Chairwoman Rosenworcel and Commissioner Carr jointly spearheaded, the FCC would ensure that the hundreds of labs and certification bodies that review and approve electronic devices for use in the U.S. are trustworthy actors that do not present national security risks, including the risk that they would do the bidding of a foreign adversary.

"Last month, the FCC took the appropriate step of denying Huawei's request for the agency to continue allowing the company's test lab to review equipment bound for the U.S. market, and we did so based on the clear national security risk that Huawei poses. Untrustworthy actors should not be participating in the FCC's equipment authorization process. But Huawei is far from the only 'Bad Lab' that has been approved to participate in the FCC's equipment authorization process—there are others with deep ties to the CCP that may pose a significant risk to the security of our networks, including entities who appear to be defense contractors for the Chinese military and even PRC-state agencies themselves," **Commissioner Carr said.** "So I am pleased we are taking the step of proposing that the test labs and certification bodies that review devices before they can be used in the U.S. are themselves trustworthy actors that we can rely on, including by barring those with risky ties to the CCP. This latest action represents another significant step in our work to strengthen our networks against risks posed by foreign adversaries. In particular, I want to thank Chairwoman Rosenworcel for her leadership and support for advancing this bipartisan initiative."

Background

- The FCC requires all electronic devices that emit radio frequencies to be certified for use in the U.S.
- This includes IoT devices, computers, fitness trackers, network gear, smartphones and baby monitors.
- Private entities—known as Telecommunication Certification Bodies (TCBs) and test labs—test tens of thousands of these devices each year and certify that they comply with various FCC rules.
- Only those TCBs and test labs recognized by the FCC can participate in the agency's process, and up to now the FCC's eligibility criteria has looked to impartiality and technical competence, rather than trustworthiness.
- In 2022, the FCC adopted rules that barred entities on the FCC's Covered List from having their devices approved for use in the U.S. due to national security risks.
- Now, the FCC's proposal will ensure that the TCBs and test labs that review equipment for use in the U.S. and compliance with FCC rules are themselves trustworthy actors.

The CCP Threat

- The People's Republic of China (PRC) leverages its control over Chinese companies and uses them to engage in surveillance and corporate espionage in the U.S., particularly in the telecommunications and technology sectors.
- As relevant here, the FCC identified a test lab in Guangdong, China affiliated with Huawei, which is on the FCC's Covered List. The FCC denied a request to renew the Huawei lab's authorization on April 30, 2024.
- Beyond this specific example, a review of the FCC's list of approved labs shows that there are others in the agency's system with deep ties to the Communist Party of China (CCP), including entities that are affiliated with Chinese state-owned-enterprises, entities that are involved in China's Military-Civil Fusion apparatus through their apparent work with the CCP's People's Liberation Army (PLA), and even entities that are themselves PRC-state actors. These labs have processed thousands of applications for devices bound for the U.S. market over the last several years.
- It is possible that other FCC-authorized TCBs and test labs may be affiliated with foreign adversary governments or entities determined by the U.S. government to pose an unacceptable security risk.

A Commonsense Proposal

- The NPRM the FCC will vote on this week seeks comment on ensuring that the TCBs and test labs that participate in the agency's equipment authorization process are trustworthy actors.
- The proposal is based on time-tested precedent. The FCC has long limited foreign control of U.S. licensees in other contexts. Furthermore, the FCC proposes to rely on official security determinations that the U.S. government has made, including the Covered List and the Defense Department's List of Chinese Military Companies.
- The NPRM explores rules to better align the rules governing TCBs and test labs with the Secure Equipment Act's provisions, which prohibit the authorization of covered equipment.
- The FCC's initiative continues the agency's bipartisan efforts to address security risks at every layer of the communications ecosystem.

###

Office of Commissioner Brendan Carr
www.fcc.gov/about/leadership/brendan-carr

Media Contact:
Greg.Watson@fcc.gov