STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *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 (May 23, 2024).

Starting with the last Administration, the United States has worked in a bipartisan manner to reorient our nation's approach to the serious threats posed by foreign adversaries. In particular, a broad cross section of lawmakers and government officials alike have been working to address the enormous risks posed by the Communist Party of China (CCP). At this point, the CCP has a well-documented record of leveraging its control over aligned companies and using them to advance the CCP's goals—from surveillance to corporate espionage and IP theft. We've seen this in spades in the telecommunications technology sectors in particular.

The FCC has played an important role in our government-wide initiative to address these types of threats. Former FCC Chairman Pai and Chairwoman Rosenworcel each deserve recognition for their work on this front. As a country, we've now taken significant actions across the entire network stack: from the device layer, to the carrier layer, to the application layer with recent action on TikTok. The FCC extends those efforts today by looking at the system the FCC relies on as part of its process for reviewing and approving electronics for use in the U.S.

To put all of this work into context—the FCC first took action at the equipment level back in 2019 by prohibiting federal USF funds from flowing towards Huawei and ZTE gear based on the clear national security risks posed by those entities.

Next, we took action at the carrier level in 2019 by moving to revoke the international Section 214 licenses of risky carriers like China Mobile, China Telecom and others with deep ties back to the CCP. At that time, I said it was time for a top to bottom review of every carrier that may be beholden to the CCP. I am pleased that those efforts have borne fruit in the FCC's subsequent bipartisan decisions to revoke additional Section 214 authorizations.

Then, after drawing attention to the "Huawei Loophole," which allowed Huawei and ZTE to continue receiving FCC approval for equipment and inserting their gear into our networks, provided that USF dollars were not used, we took action that prohibits those entities on our Covered List from receiving FCC equipment approval.

Most recently, Congress took perhaps the most significant action to date by enacting legislation requiring TikTok to break up with the CCP.

While each of those individual decisions worked to address a specific threat, collectively, they show that America has the resolve to stand up to the CCP's aggression.

Now, we propose to take another important step forward in securing our communications networks. This proposal, which I have been pleased to work on alongside Chairwoman Rosenworcel, will ensure that the test labs and certification bodies (TCBs) that review electronic devices for compliance with the FCC's equipment authorization rules are trustworthy actors that the FCC can rely on. Despite their relatively low public profile, these entities play an important role in evaluating whether electronic devices that emit radio frequencies (RF) operate effectively and meet other FCC requirements before they

can be certified for use in the U.S. This covers a broad swath of consumer electronics from IoT devices, smartphones, fitness trackers, and baby monitors to network equipment like routers and base stations.

Historically, the FCC's eligibility criteria for test labs and TCBs has looked to impartiality and technical competence, rather than focusing on factors that are relevant to national security concerns. But the need for this type of review has increased in recent years. Indeed, 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. And we have expressed concern about white labeling devices—meaning, that someone slaps a new name on Huawei gear in an effort to sneak it through the equipment authorization process.

So to complement our efforts on this front, the FCC's proposal today 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.

Our concerns are well-founded. After identifying a test lab in Guangdong, China affiliated with Huawei, the FCC rejected a request to renew the lab's authorization on April 30th. Correctly so. But a further review of the FCC's list of approved test labs[1] reveals other entities with deep and concerning ties back to the CCP. The list includes entities that are affiliated with Chinese state-owned-enterprises; entities that appear to play a role in supporting the CCP's People's Liberation Army; as well as some PRC government agencies themselves. FCC records indicate those labs have processed thousands of applications for U.S.-bound devices 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.

Our initiative is based on time-tested precedent, too. 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 Department of Commerce's Entity List and the Defense Department's List of Chinese Military Companies (1260H List). We also explore regulations that could better align our rules governing TCBs and test labs with the Secure Equipment Act's provisions, which prohibit the authorization of covered equipment. So for my part, I am grateful to the Chairwoman for moving this proposal forward. It has my strong support.

Finally, I would like to thank the many staff from the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau for their thorough work on this item. I'm grateful for all of their hard work and collaboration on this initiative.

[1] A full list of test labs that are currently accredited by the FCC can be found here: https://apps.fcc.gov/oetcf/eas/reports/TestFirmSearch.cfm