STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

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).

Our wireless future is about connecting everything. It is about opening up possibilities for connectivity that we cannot even fully imagine today. By exponentially increasing the connections between people and things around us, wireless technologies are set to become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more.

At the Federal Communications Commission, we have a front row seat. Every day we get to see how these innovations are changing our world. We also see how important it is that every one of these connections is secure.

For decades, the FCC equipment authorization program has been a vital part of ensuring the safety of radiofrequency devices in the United States. In fact, we process more than 30,000 new device authorizations every year, resulting in millions of new wireless products. That's a lot of Wi-Fi routers, sensors, smartphones, and baby monitors. We check them, and other devices that connect using our airwaves, to make sure that they do so safely, without harmful interference, and in a manner that complies with our rules.

To keep this process moving along, the FCC has authorized the use of Telecommunications Certification Bodies, or TCBs. That means innovators bring their new devices to test labs that produce technical reports assessing their products. Then they take those reports to TCBs. The TCBs, in turn, evaluate this information and determine if the new devices comply with FCC rules. If they do, the TCB can certify the device under the equipment authorization program.

This process has worked well. But as the number of wireless connections around us multiply and the importance of the security of those connections matters more than ever before, this system needs an update. That is what we propose here today.

This action is part of a broader effort at this agency to make network security a priority. For the first time in history, we have revoked the authorization of Chinese state-affiliated carriers that have been identified as a national security threat. We have built a first-of-its-kind program to remove insecure foreign equipment from our nation's communications networks. We have revamped our policies for assessing the security of proposed undersea cables for the first time in twenty years. We are proposing new measures to address the insecurities in Border Gateway Protocol, which can be used by malicious foreign actors to hijack internet traffic. On top of that, we now publish and update a Covered List of communications equipment and services that pose an unacceptable risk to national security. We exclude this equipment from our universal service programs. We also prevent its processing in our equipment authorization program.

With these efforts in the background, in this rulemaking we do three key things to update our security policies and practices with respect to TCBs and test labs. First, we propose to prohibit all entities on the Covered List from owning or controlling TCBs or test labs. As part of this effort, we have already suspended the approval of a test lab operated by Huawei and flagged for our national security colleagues other labs with possible ties to the government of the People's Republic of China. Second, we seek comment on prohibiting the recognition of TCBs and test labs owned or controlled by a foreign adversary or any other entity that has been found to pose a risk by national security agencies. Third, to implement these changes we propose to collect information on the ownership and control of TCBs and test labs.

The pace at which we are seeing new technologies that depend on wireless connections helped spur this effort. But so did a recommendation from Commissioner Carr, who rightfully and thoughtfully suggested that our practices needed an update. I want to thank him for his close collaboration. Our equipment authorization program will be more secure because of it.

Thank you also to my other colleagues and to the staff who worked on this rulemaking, including Reza Biazaran, Jamie Coleman, David Duarte, Paul Murray, Siobahn Philemon, Ron Repasi, Dana Shaffer, Ross Slutsky, Jim Szeliga, George Tannahill, and Krista Witanowski from the Office of Engineering and Technology; Justin Cain, Michael Connolly, David Furth, Jessica Hynosky, Debra Jordan, Zenji Nakazawa, Sonja Rodriguez, and Jim Schlichting from the Public Safety and Homeland Security Bureau; Saurbh Chhabra, Lloyd Coward, Susan Mort, and Roger Noel from the Wireless Telecommunications Bureau; Shannon Lipp and Jeremy Marcus from the Enforcement Bureau; Patrick Brogan, Rachel Kazen, Cher Li, Ken Lynch, Catherine Matraves, Mark Montano, Erik Salovaara, Michelle Schaefer, Donald Stockdale, Patrick Sun, and Emily Talaga from the Office of Economics and Analytics; Edward Carlson, Jared Carlson, Denise Coca, Kathleen Collins, Olga Madruga-Forti, Nese Guendelsberger, Francis Gutierrez, Gabrielle Kim, David Krech, Ethan Lucarelli, Brandon Moss, and Thomas Sullivan from the Office of International Affairs; Michael Gussow and Joy Ragsdale from the Office of Communications Business Opportunities; and Marlene Dortch and Katura Jackson from the Office of the Secretary.