Statement of
Commissioner Geoffrey Starks

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).

Electronic devices, or in FCC parlance, Radio Frequency (RF) devices -- from cell phones to computers, baby monitors, garage openers, and televisions -- are an integral part of our daily lives. Before these devices reach where we live, work and play, our rules require RF devices to be properly authorized. These rules ensure that RF devices operate effectively without causing harmful interference and otherwise comply with our FCC requirements.

Over the last several years we have undertaken significant efforts to protect the security of our communications networks and devices. We updated our equipment authorization rules to prohibit authorization of communications equipment identified on our Covered List. By stopping equipment identified as a threat to the United States from entering our markets we decreased the risk that it can be used against us.

Today, I'm glad to support our proposal to update our rules governing Telecommunications Certification Bodies (TCBs) and test labs to further protect Americans and ensure that our equipment authorization processes are not undermined by the very entities that help us to enforce them.

TCBs and test labs play a critical role in approving tens of thousands of equipment authorizations every year, and they are located all over the world. TCBs and test labs help ensure that equipment we approve complies with our rules and regulations and that any prohibited equipment is kept out of our nation's supply chain. They are an important line of defense against improper and insecure equipment. To that end, TCBs and test labs acting on our behalf must also be trustworthy, impartial, and free from influence. Their ability to do so may be compromised if they are associated with any untrustworthy entity or adversarial state that seeks to compromise our networks or communications supply chain.

Notably, this proposal is consistent with our recent efforts to create the Cyber Trust Mark. There, we actually highlighted the importance of test labs to ensure that IoT devices receiving the mark are not compromised. As the record develops, I am open and eager to review any comments on how these proposed changes may affect the overall ecosystem for devices, including with regard to the Mutual Recognition Agreements we have negotiated throughout the world aimed at creating a standardized global approach to conformity assessments.

I thank the fantastic FCC staff for their hard work on this important proceeding. This item has my strong support.