September 11, 2025

Marlene H. Dortch, Esq.
Secretary
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*

Dear Ms. Dortch:

On behalf of the undersigned trade associations representing a broad cross-section of America's technology, manufacturing, and communications industries, we respectfully write in response to the Commission's Further Notice of Proposed Rulemaking (FNPRM) in the above-referenced proceeding.[1]

Our organizations share the Commission's goal of enhancing the integrity of the equipment authorization program and protecting national security. However, several of the proposals in the FNPRM risk imposing significant costs and disruptions on U.S. companies and consumers without delivering commensurate security benefits. We urge the Commission to take a measured approach that safeguards security while preserving innovation, consumer choice, and supply chain resilience.

Avoid Overbroad Prohibitions

Banning testing facilities or certification bodies based solely on their physical location, rather than on evidence of ownership or control by a prohibited entity, would unnecessarily reduce global testing capacity. Such an approach could delay introduction of life-enhancing and economy-invigorating innovations, raise costs, deter investment and invite reciprocal restrictions on U.S. companies abroad. Commenters who suggest the rules go further to restrict *any* non-U.S.-owned Telecommunications Certification Bodies (TCBs) or labs promote short-sighted commercial interests at the expense of a robust,

[1] *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, Report and Order and Further Notice of Proposed Rulemaking, ET Docket No. 24-136, FCC 25-27 (rel. May 27, 2025).

procompetitive market for equipment authorization capable of supporting the growing global technology sector. Instead, a targeted, evidence-based standard is essential to avoid trade conflicts, unintended harms to U.S. global competitiveness and leadership, and ensure alignment with the widely supported view that cyber and supply chain security is critical to the security of consumers and businesses alike.

Preserve the Role of TCBs and Testing Labs

Proposals to require third parties to duplicate or second-guess the work of accredited TCBs would impose needless expense and slow product certification. Such proposals also ignore the reality that some TCBs could have competitive incentives to hamstring the work done by others. Similarly, restricting relationships between TCBs and test labs would disrupt established practices that have long ensured impartiality and efficiency, and would likely raise costs of those seeking to have their devices tested. Existing international accreditation systems already provide rigorous safeguards to uphold integrity.

Protect the Supplier's Declaration of Conformity (SDoC) Program

As many commenters – including U.S.-based laboratories and manufacturers – note, the SDoC process has proven effective for low-risk devices, balancing oversight with efficiency. Requiring all SDoC devices to be tested by FCC-accredited labs would create costly bottlenecks, reduce available testing capacity, and delay market entry of consumer technologies without clear evidence of improved security.

Ensure Sufficient Transition Periods and Clear Guidance

Commenters broadly agree – whether in favor of or opposed to the proposed changes in the FNPRM – that should the FCC determine that any changes to the rules are warranted, adequate time must be allowed for industry to comply and adjust supply chains. Abrupt implementation would force manufacturers to break contracts, miss product launch windows, and delay the availability of innovative products for American consumers. Clear FCC guidance on transition procedures will be critical to minimizing confusion and disruption.

Conclusion

Our industries remain committed partners in strengthening the security of America's communications networks and ensuring the integrity of the equipment authorization program. We urge the Commission to avoid overly broad or duplicative requirements that would slow innovation, raise costs for consumers, and undermine the global competitiveness of U.S. companies. Instead, the Commission should focus on targeted, evidence-based measures that meaningfully enhance security while supporting the continued success of the equipment authorization program.

Sincerely,

Sriram Gopal
Senior Director, Regulatory Policy & Circular Economy
Association of Home Appliance Manufacturers (AHAM)

J. David Grossman
Vice President, Policy & Regulatory Affairs
Consumer Technology Association (CTA)

Christopher L. Shipley
Executive Director of Public Policy
INCOMPAS

Sameer Boray
Senior Policy Manager, Trust, Data and Technology
Information Technology Industry Council (ITI)

Alex Baker
Director, Regulatory & Industry Affairs
National Electrical Manufacturers Association (NEMA)

Colin Andrews
Senior Director, Government Affairs
Telecommunications Industry Association (TIA)