Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
	)	
	)	

COMMENTS OF
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA") respectfully submits these comments to the Federal Communications Commission ("Commission" or "FCC") in response to the Second Further Notice of Proposed Rulemaking ("*Second FNPRM*") in the above-captioned proceeding.[1] As a U.S.-based trade association and standards development organization representing more than 400 trusted, global manufacturers of telecommunications equipment and services, TIA offers the following comments to support the Commission's consistent and effective implementation of national security policy.

I. INTRODUCTION AND SUMMARY

Ensuring the trustworthiness of information and communications technology ("ICT") suppliers and the resiliency of ICT networks is a core mission for TIA.[2] TIA and its members

[1] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 25-71 (rel. Oct. 29, 2025) ("*Second Order*" or "*Second FNPRM*").

[2] TIA actively advances trusted suppliers through standards development and certification. TIA developed and administers SCS 9001, a comprehensive system for global supply chain security management. *See* Mike Regan, *TIA's SCS 9001 Cyber and Supply Chain Security Standard – Update*, NIST (Jan. 2023), https://csrc.nist.gov/csrc/media/Presentations/2023/tia-quest-forum-scs-9001-update/images-media/Jan-24-2023-ssca-regan.pdf. TIA recently launched the development of a new Data Center Quality Standard, which will draw on TIA's decades of leadership through the QuEST Forum and over 20 years of empirical field data and proven quality system methodologies to address reliability, sustainability, and performance across evolving supply chains. *See* Press Release, TIA, TIA Launches Data Center Quality Standard Initiative (Oct. 8, 2025), https://tiaonline.org/press-release/telecommunications-industry-association-tia-launches-data-center-quality-standard-initiative/.

have long supported the Commission's work to consistently and effectively implement the Secure Networks Act and Secure Equipment Act.[3] As the Commission considers additional steps to implement this complex, novel regulatory framework, it should ensure that any restrictions on equipment or services from untrusted suppliers directly reflect specific determinations from sources enumerated in the Secure Networks Act ("Enumerated Sources"), including with respect to the scope and timeline(s) for restrictions on component parts. Where the Commission exercises discretion, any restrictions on components should (i) reflect a targeted, risk-based approach that leverages input from Enumerated Sources, (ii) include reasonable transition periods based on the production cycles of impacted products, and (iii) be accompanied by clear, workable guidance for compliance.

II. DIRECTLY REFLECTING SPECIFIC DETERMINATIONS BY ENUMERATED SOURCES WILL ENSURE A CONSISTENT NATIONAL SECURITY POSTURE AND REDUCE COMPLIANCE CHALLENGES.

The question of whether and how to impose restrictions on components that fall within the scope of equipment and services included on the FCC's Covered List poses complex challenges that future updates to the Covered List will likely continue to raise. Ensuring that any prohibition on components directly reflects the specific determination on which it is based – including with respect to scope and timeline – will help ensure that the FCC's Covered List implementation remains aligned with the rest of the federal government's national security posture, consistent with the Secure Networks Act. This in turn will reduce compliance

[3] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) ("Secure Networks Act"); Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 (Statutory Notes and Related Subsidiaries)) ("Secure Equipment Act"). *See, e.g.*, Comments of TIA, ET Docket No. 21-232 & 21-233 (Sept. 20, 2021); Reply Comments of TIA, ET Docket No. 21-232 & 21-233 (Oct. 18, 2021); Comments of TIA, ET Docket Nos. 21-232 & 21-233, (Apr. 7, 2023); Reply Comments of TIA, ET Docket No. 21-232 & 21-233 (May 8, 2023) ("TIA EA FNPRM Reply Comments").

challenges for entities working to meet both the FCC's requirements and those of other agencies implementing restrictions on untrusted suppliers.

In passing the Secure Networks Act and the Secure Equipment Act, Congress clearly articulated the FCC's role in addressing untrusted ICT suppliers: namely, (1) establishing and maintaining the Covered List based on national security determinations by Enumerated Sources; and (2) prohibiting equipment and services on the Covered List from receiving FCC subsidies or equipment authorization. The Secure Networks Act directs the Commission to rely on a "specific determination" from an Enumerated Source to update the Covered List.[4] As the Commission noted in the *Second Order*, so far Congress has passed "one narrow exception to this exclusivity" by "directing the Commission to add certain communications equipment and services related to Unmanned Aircraft Systems to the Covered List in the event that no appropriate national security agency makes a specific determination within one year of enactment, i.e. December 23, 2025."[5] Congress also made clear that it expects the Covered List to continuously reflect the determinations of Enumerated Sources, including with respect to products that do not belong on the Covered List.[6]

With that in mind, any national security prohibitions on equipment or services – including components – from untrusted suppliers should directly flow from specific determinations by Enumerated Sources. As Enumerated Sources provide increasing levels of

[4] Secure Networks Act § 2(c) (directing the FCC to place on the Covered List "any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on" expressly named sources in law or according to "specific determinations" made by expressly named parts of the Executive Branch).

[5] *Second Order* ¶ 5, n.4 (citing National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, § 1709(a)(2) (2024)).

[6] *See*, *e.g.*, H.R. Report No. 116-352 (2019) ("The Committee expects that the FCC will monitor these [Enumerated] sources, *both for purposes of adding* covered equipment and services to the list *and removing* equipment and services that are no longer considered covered equipment or services by the source cited in making the original determination.") (emphasis added).

specificity regarding the scope of products covered by a specific determination, that specificity – which reflects a careful balancing of national security risk and economic/supply chain impact – should guide the Commission's application of prohibitions on components.[7] For example, the high-level language in the FY19 National Defense Authorization Act Section 889 gives the FCC broad discretion to impose prohibitions on "telecommunications equipment produced by" Huawei or ZTE.[8] Any prohibitions on components should only include those components that fall within the scope of a specific determination.

III. ANY COMPONENT RESTRICTIONS SHOULD BE TARGETED, RISK-BASED, INFORMED BY ENUMERATED SOURCES, AND ACCOMPANIED BY REASONABLE TRANSITION PERIODS AND CLEAR COMPLIANCE GUIDANCE.

Where the Commission exercises its own discretion regarding which components "would render the relevant device covered equipment," a targeted, risk-based approach informed by input from Enumerated Sources can help ensure a consistent national security posture and reduce burdens on trusted manufacturers working to comply. Adopting reasonable transition periods that reflect the diverse, complex, and global nature of supply chains impacted by a particular prohibition will reduce negative economic impacts and support continued U.S. leadership in the international technology ecosystem. Finally, working with stakeholders to develop clear guidance for implementing any component-level prohibitions will promote consistent

[7] As the Commission explained in the *Second Order*, in certain instances other factors may outweigh national security risks. *Second Order* ¶ 46 (discussing one such instance in the Commerce Department's Connected Vehicles Rule, where the Bureau of Industry and Security adopted exemptions and delayed the effectiveness of its rule "determining the scope of the prohibitions required a balancing of the need to address the undue or unacceptable risk posed by foreign adversary involvement in the connected vehicles supply chain with the impact on the public and industry.").

[8] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1918 (2018) ("FY19 National Defense Authorization Act").

compliance across diverse products and reduce administrative burdens on both trusted manufacturers and the equipment authorization program itself.

a. A Targeted, Risk-Based Approach Leveraging Input from Enumerated Sources Will Ensure Consistent Implementation of National Security Rules.

As TIA has underscored throughout the FCC's Secure Equipment Act implementation, a targeted, risk-based approach to prohibiting components, grounded in the specific determinations of Enumerated Sources, will best ensure that the Commission's rules remain aligned to the rest of the federal government's and reduce burdens on trusted manufacturers working to comply.[9] Overbroad component level restrictions could unintentionally favor vendors from foreign adversaries with flexible and opaque supply chains, undermining U.S. and allied industry competitiveness. We appreciate the Commission's aim to strike the right balance in this regard, particularly its intention to identify components with sufficient specificity, its interest in options to help reduce compliance burdens, and its recognition that the availability of some replacement parts may be limited.[10] In addition to adopting reasonable transition periods and developing clear guidance (discussed below), the Commission can help by avoiding restrictions on components that do not actually pose national security risk, such as a logic-bearing component that does not provide the ability to exfiltrate sensitive information or disrupt the function of the product. In other words, any restrictions on components should focus on the capability-based risk of that component.

Close collaboration with Enumerated Sources can help inform the Commission's risk analysis regarding the scope of components that pose an unacceptable national security risk. As

[9] *See* TIA EA FNPRM Reply Comments at 4-6 (encouraging the Commission to take a targeted, risk-based approach to components with clear, workable guidance for compliance).

[10] *Second FNPRM* ¶ 59.

TIA and CTA underscored in their recent Petition for Clarification, any final decision regarding the scope of Covered List prohibitions should incorporate input from Enumerated Sources to the extent provided.[11] TIA encourages the Commission to explore potential partnership with Enumerated Sources for this purpose.[12]

The Commission should also take a risk-based approach to enforcing these restrictions that ensures compliance burdens bring commensurate security benefits. As stakeholders have previously urged, any attestation requirements should rely on an applicant's reasonable investigation into the supply chain and allow applicants to rely on the attestations of their suppliers.[13] In addition, the Commission should foster consistent administration through updated training for telecommunications certification bodies and FCC-approved laboratories, periodic checks for decision consistency, and clear channels to challenge component reviews where appropriate.

b. Reasonable Transition Periods Based on Impacted Production Cycles Will Reduce Economic Impacts and Support Continued U.S. Leadership.

To minimize negative impacts on U.S. consumers and businesses, any restrictions on components should include reasonable transition periods that reflect the production cycles of impacted products. To find suitable alternatives to newly prohibited components, manufacturers need time to source, test, and integrate new parts into their products. This process can take more or less time depending on the nature of the component and the complexity of the final product. For example, through close collaboration with automakers, the Department of Commerce recognized the need to provide two years for connected vehicle manufacturers to replace certain

[11] Petition for Clarification of the Consumer Technology Association and the Telecommunications Industry Association, ET Docket No. 21-232, at 6 (Dec. 22, 2025).

[12] *Second FNPRM* ¶ 65.

[13] *See* TIA EA FNPRM Reply Comments at 5-6.

software components and five years for certain hardware components.[14] The Commission may face a similar situation regarding component restrictions. It may also need to consider disparate impacts as the same types of ICT components often supply a variety of products across diverse sectors with different multi-year production cycles. If all manufacturers must find alternative factories with the capability to produce at scale, the time to market will increase significantly. In some cases, factories for alternative components may need to be built before they can begin producing equipment. Any component restrictions that the Commission adopts should provide sufficient time for manufacturers to source alternatives so that manufacturers can continue to meet the needs of U.S. consumers and remain competitive in the global market.

c. Collaborating with Trusted Manufacturers to Develop Clear Guidance Will Promote Consistent Compliance and Reduce Administrative Burdens.

Finally, working with impacted stakeholders to develop clear, workable guidance will significantly reduce compliance burdens associated with prohibitions on components. As TIA and CTA requested in their recent Petition regarding the term "produced by," a collaborative process will allow manufacturers to bring more specific questions to Commission staff and problem-solve real-world challenges.[15] This could be accomplished through a Public Notice seeking public comment, a roundtable discussion, a multistakeholder committee workstream (such as the Technological Advisory Council or other group established under the Federal Advisory Committee Act), or some combination of these mechanisms.

[14] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360 (Jan. 16, 2025); 15 C.F.R. § 791.300, et seq.

[15] CTA-TIA Petition for Clarification at 7.

IV. CONCLUSION

TIA and its members appreciate the Commission's work to faithfully implement the Secure Equipment Act in a manner that promotes effective compliance and minimizes burdens on trusted manufacturers. The Commission can best achieve this goal by ensuring that any restrictions on equipment or services from untrusted suppliers – including components – directly reflect specific determinations from Enumerated Sources. Where the Commission exercises discretion, any restrictions on components should (i) reflect a targeted, risk-based approach that leverages input from Enumerated Sources, (ii) include reasonable transition periods based on the production cycles of impacted products, and (iii) be accompanied by clear, workable guidance for compliance. TIA welcomes continued engagement with the Commission in support of this strategic imperative.

/s/ *Melissa Newman*
Melissa Newman
Senior Vice President

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Blvd, Floor 25
Arlington, VA 22209
(703) 907-7700

January 5, 2026