

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

PETITION FOR CLARIFICATION

Consumer Technology Association (CTA)¹ and the Telecommunications Industry Association (TIA)² (collectively “the Associations”) respectfully submit this petition for clarification of two discrete elements of the *Second Report and Order (Second Order)* in the above-captioned proceeding.³ The changes discussed below will align the Commission’s next steps with Congress’s directives and ensure more faithful compliance with the FCC’s rules going forward.

INTRODUCTION AND SUMMARY

CTA and TIA appreciate the Federal Communications Commission’s (“FCC’s” or “Commission’s”) continued work to implement the Secure and Trusted Communications

¹ As North America’s largest technology trade association, CTA® is the tech sector. Our members are the world’s leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most powerful tech event in the world.

² As a U.S.-based trade association and Standards Developing Organization, TIA represents more than 400 trusted, global manufacturers of telecommunications equipment and services. TIA members design, produce, market, and manage the ICT equipment and services that connect Americans and our partners around the world to high-speed broadband networks.

³ 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*).

Networks Act (Secure Networks Act) and the Secure Equipment Act.⁴ Our associations share the Commission’s commitment to protecting information and communications technology (ICT) supply chains from equipment and services that threaten the nation’s security, and we recognize the complex challenges that the FCC faces in implementing these novel and evolving rules. CTA and TIA are committed to helping the Commission implement these rules as effectively as possible and to ensuring our members—who together represent a vast range of technology suppliers across nearly every sector of the economy—can comply fully and consistently.

Having contributed to the FCC’s implementation of the Secure Equipment Act at previous stages,⁵ CTA and TIA seek two targeted clarifications in the *Second Order*.

Specifically:

- (1) Direction in FCC rule text that any actions under the new process for limiting existing authorizations are taken in a way that directly reflects specific determinations by national security sources enumerated in the Secure Networks Act (Enumerated Sources); and
- (2) Direction to the Public Safety and Homeland Security Bureau (PSHSB) and the Office of Engineering and Technology (OET) to engage with stakeholders in developing further guidance on how to evaluate whether a product is “produced by” a specified entity.

⁴ 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).

⁵ See, e.g., Comments of the Consumer Technology Association (CTA), ET Docket Nos. 21-232 & 21-233 (Sept. 20, 2021); Comments of the Telecommunications Industry Association (TIA), ET Docket No. 21-232 & 21-233 (Sept. 20, 2021); Letter from ACT – the App Association, CTA; Council to Secure the Digital Economy, CTIA, Internet Association, Information Technology Industry Council, U.S. Chamber of Commerce, and USTelecom to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232 (Sept. 20, 2021); Reply Comments of CTA, ET Docket Nos. 21-232 & 21-233 (Oct. 18, 2021); Reply Comments of the TIA, ET Docket No. 21-232 & 21-233 (Oct. 18, 2021); Comments of CTA, ET Docket No. 21-232 & 21-233 (Apr. 7, 2023); Comments of TIA, ET Docket Nos. 21-232 & 21-233, (Apr. 7, 2023); Reply Comments of CTA, ET Docket Nos. 21-232 & 21-233 (May 8, 2023); Reply Comments of the TIA, ET Docket No. 21-232 & 21-233 (May 8, 2023).

Together, these adjustments will significantly help the Commission ensure that ongoing implementation of the Secure Equipment Act remains aligned to the United States’ overarching risk posture and help reduce costs and uncertainty facing trusted manufacturers as they work to comply with these evolving rules. CTA and TIA appreciate the Commission’s consideration and welcome further engagement regarding these requests.

I. ANY LIMITATIONS ON EXISTING AUTHORIZATIONS OF COVERED EQUIPMENT SHOULD DIRECTLY REFLECT ITS SOURCE-SPECIFIC DETERMINATION

The Commission correctly recognized that retroactive application of Covered List prohibitions poses complex implementation challenges and adopted a prospective approach to ensure restrictions on existing authorization are added only where absolutely required and with great care.⁶ The Associations appreciate the Commission’s effort to craft an approach “to effectively address the established national security risks posed by previously authorized covered equipment while minimizing the impact on users.”⁷ To ensure consistency with the Secure Networks Act and in the application of these prohibitions, the Associations agree that the relevant “specific determination must be the centerpiece of OET and PSHSB’s analysis” about whether and how to limit an existing authorization.⁸ To avoid potential conflict between the Commission’s implementation and increasingly detailed actions by Enumerated Sources, the

⁶ See *Second Order* ¶¶ 33-50. The Commission explained that “rather than favoring sweeping revocations that would require the removal and replacement of equipment,” it adopted a prospective approach to reduce excessive burdens on complying entities. *Id.* Appendix C ¶ 16.

⁷ *Id.* ¶ 32. Stakeholders have consistently emphasized, and lessons learned throughout implementation of the Supply Chain Reimbursement Program have taught, that retroactive application of Covered List prohibitions are extremely costly, complicated, and can pose prohibitive challenges for smaller entities. See *id.* ¶ 36. Future determinations by Enumerated Sources may address equipment permeating throughout a broader set of stakeholders in the market and engage in more granular assessment of components—compounding the challenges of retroactively applying restrictions to authorized devices.

⁸ *Id.* ¶ 47.

Commission’s rules should specify that any limitations on existing authorizations must *directly reflect* the underlying specific determination(s).

The Associations also urge the Commission to closely coordinate with relevant Enumerated Sources before considering limiting existing authorizations. Given that Congress invested the Enumerated Sources with the responsibility to make the specific determinations underlying the FCC Covered List, the Commission and Bureaus acting on delegated authority should accept and incorporate formal input from an Enumerated Source into any final decision.

**A. Directly Reflecting Specific Determinations in Covered List
Implementation Ensures a Whole-of-Government Approach and
Supports Private Sector Compliance**

In the Secure Networks Act, Congress explicitly directed the Commission to populate the Covered List with specific determinations from national security sources whose mission, resources, and structure provide the requisite information and ability to weigh complex national security risks against economic impact and other concerns.⁹ Since enactment, the specific determinations by Enumerated Sources have provided increasing specificity by including details about the scope of products covered and appropriate timelines for implementation.¹⁰ They have carefully weighed national security risk, economic and supply chain impact and other factors, developed in consultation with industry stakeholders.

⁹ 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).

¹⁰ See, e.g., DHS, *BOD 17-01: Removal of Kaspersky-branded Products* (Sept. 17, 2017), <https://www.cisa.gov/news-events/directives/bod-17-01-removal-kaspersky-branded-products>; Department of Commerce, Bureau of Industry and Security, Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc., 89 Fed. Reg. 52434 (June 24, 2024).

The Commission’s implementation of Covered List prohibitions should directly reflect these specifications. As many commenters emphasized in response to the FCC’s proposal to incorporate the Department of Commerce Connected Vehicles Rule into the Covered List,¹¹ deviating from these important, carefully balanced scope, timelines and flexibilities would lead to misalignment between the Commission’s implementation and that of other agencies.¹² Such misalignment would undermine the Administration’s policy goals and create unnecessary and inconsistent regulatory burdens for manufacturers and suppliers when they are already navigating unprecedented geopolitical, economic, and regulatory challenges. Conversely, ensuring in the FCC’s rules that any updates to, or limitations on, existing authorizations must directly reflect the underlying specific determination(s) will help ensure that the FCC’s implementation remains consistent with the rest of the U.S. government’s national security posture and help provide clarity for businesses as they comply with the Commission’s rules.

B. Surgical Edits to the FCC’s Rules Will Ensure Alignment Between Commission or Bureau Action and a Relevant Specific Determination

The Associations request that the codified rule language mirror the *Second Order*’s holding that potential limitations of existing authorizations “will primarily rely upon the details of the relevant specific determination(s) used to inform a given entry on the Covered List.”¹³ Specifically, in § 2.939(e)(2), the Associations respectfully ask the Commission to modify the rule text as follows:

¹¹ *The Public Safety and Homeland Security Bureau and the Office of Engineering and Technology Seek Public Input on Commerce Department Determination Regarding Certain Connected Vehicle Technologies*, WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233, Public Notice, DA 25-418 (PSHSB/OET May 23, 2025).

¹² *See, e.g.*, 5G Automotive Association, et al., to Brendan Carr, Chairman, FCC, and Jeffrey Kessler, Under Secretary of Commerce for Industry and Security, WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233 (Sept. 4, 2025).

¹³ *Second Order* ¶ 45.

The public notice will include an assessment of the impact of the proposed prohibition with consideration of public interest factors, including: the unacceptable risks the equipment was found to pose, the economic and supply chain impacts, and any other criteria as specified by the Commission. The public notice should directly reflect ~~give particular weight to~~ the specific determination(s), and any accompanying rules or analyses, through which the relevant equipment was added to the Covered List.

Taking this step will enshrine concrete language requiring that any such limitation must *directly reflect* a relevant determination.

Should PSHSB and OET find it necessary to weigh the national security risk of allowing existing authorizations against the potential economic impact of limiting those authorizations, the Commission should closely coordinate with the relevant Enumerated Sources before making any decision. In the event that Enumerated Sources provide formal input, the Bureaus and Commission should incorporate that input into any final decision.

II. FURTHER STAKEHOLDER INPUT TO DEFINE “PRODUCED BY” WILL SUPPORT NATIONAL SECURITY AND REDUCE COMPLIANCE BURDENS

Trusted suppliers share the U.S. government’s commitment to ensuring the trustworthiness of their products and manufacturers work with partners throughout their global supply chains to comply with limitations or prohibitions adopted in response to the evolving national security landscape. Among other things, manufacturers need a clear understanding of whether equipment is “produced by” a specified entity to fulfill their end of this partnership.¹⁴ Despite the Commission’s responsiveness to the request to clarify “ambiguity surrounding the term ‘produced by’ in the context of covered equipment,”¹⁵ members continue to express concerns about translating the *Second Order* into practical guidance for their supply chain

¹⁴ *Id.* ¶ 51 (explaining that for responsible parties and applicants for equipment authorization to comply with the Covered List prohibited, they must assess their equipment and determine the equipment is not “produced by” a prohibited Covered List entity).

¹⁵ *Id.* ¶ 52 (quoting a commenter request).

teams.¹⁶ Specifically, manufacturers anticipate challenges implementing the discussion in the *Second Order* that “whether a device is produced by a particular entity could be based on multiple factors or the totality of circumstances, particularly when considering the role played by multiple entities to bring a device into existence” and future listings “may use different language that indicates an intent to capture a larger or smaller set of communications equipment.”¹⁷ Manufacturers will need further clarity as they consider questions, for example, regarding what level of involvement an entity must have in the production of software components to be considered a producer.

Recognizing the complexity of this question and the Commission’s imperative not to adopt a potentially underinclusive or ill-fitting definition, the Associations request that the FCC work with stakeholders to develop guidance on interpreting the term “produced by.” A collaborative process will allow manufacturers to bring more specific questions to Commission staff and problem-solve real-world challenges. This could be accomplished through a Public Notice seeking public comment, roundtable discussion, a multistakeholder committee workstream, or some combination of these mechanisms.

CONCLUSION

The Commission, CTA, TIA, and our members share a common goal of ensuring trustworthy communications across America’s networks. The requested clarifications above will help ensure that the FCC’s execution of its duties under the Secure Networks Act and Secure Equipment Act perpetuate a consistent national security risk posture across the U.S. government

¹⁶ *Id.* ¶ 53 (holding that “when carrying out their responsibilities associated with the prohibition on authorization of covered equipment under section 2.903(a), or any of the required attestations related to covered equipment, applicants, responsible parties, and entities named in their reporting obligations should take a broad view of the term ‘produced by’”) (footnotes omitted).

¹⁷ *Id.*

and help reduce burdens on trusted suppliers complying with this ever-evolving set of rules to the benefit of U.S. economic and technological leadership. CTA and TIA appreciate the FCC's work to implement these rules accordingly and welcome further engagement as the Commission considers this Petition.

Respectfully submitted,

/s/ J. David Grossman

J. David Grossman
Vice President, Policy & Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

December 22, 2025

/s/ Melissa Newman

Melissa Newman
Senior Vice President

Telecommunications Industry Association
1201 Wilson Blvd, Floor 25
Arlington, VA 22209