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 CONSUMER TECHNOLOGY ASSOCIATION

J. David Grossman
Vice President, Policy & Regulatory Affairs

Rachel Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

January 5, 2026

TABLE OF CONTENTS

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
CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association (CTA)[1] respectfully submits these comments in response to the Federal Communications Commission's ("Commission's" or "FCC's") Second Further Notice of Proposed Rulemaking in the above-captioned proceeding.[2] CTA recognizes that cybersecurity is both a consumer and national security issue and suggests ways to meet the Commission's national security goals while ensuring consumers continue to have access to innovative, trusted devices.

I. INTRODUCTION AND SUMMARY

CTA and its members support the Commission's goal of enhancing device security and protecting the U.S. technology supply chain while preserving a competitive, innovative technology market, for the benefit of consumers and businesses alike.[3] An active partner

[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] *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, ET Docket No. 21-232, FCC 25-71 (rel. Oct. 29, 2025) ("*Second Order*" or "*Second FNPRM*").

[3] For example, CTA has been a champion and one of the leading associations working with the FCC to develop the Internet of Things Cybersecurity Labeling Program to administer the U.S. Cyber Trust Mark. *See*, *e.g.*, J. David Grossman, *Aligning Strategy with Action: The Case for the U.S. Cyber Trust Mark*, LinkedIn (Dec. 18, 2025), https://www.linkedin.com/pulse/aligning-strategy-action-case-us-cyber-trust-

throughout this proceeding,[4] CTA continues to support the Commission's work to implement the complex and novel regulatory framework established by the Secure Networks Act and Secure Equipment Act.[5] Through this process, the Commission plays a critical and specific role within the U.S. government's overarching implementation of national security policy.

As the Commission considers next steps regarding questions raised in the *Second FNPRM*, CTA offers the following recommendations so this process both (i) maintains a consistent national security approach across the federal government and the wide array of impacted sectors, and (ii) supports effective implementation of these evolving rules while minimizing unnecessary costs and unintended consequences. Specifically, CTA requests that any Covered List update and prohibition based on that update directly reflect the underlying specific determination by an enumerated source in the Secure Networks Act (Enumerated Source), including for the scope of products covered and timeline for implementation. Where the FCC exercises discretion in extending Covered List prohibitions to component parts, such discretion should (i) take a targeted, risk-based approach based on functionality, (ii) integrate any formal input provided by a relevant Enumerated Source, (iii) work with stakeholders to provide clarity

---

mark-j-david-grossman-gxyye; J. David Grossman, *The U.S. Cyber Trust Mark: Empowering Consumers & Manufacturers for a More Secure America*, LinkedIn (Apr. 17, 2025), https://www.linkedin.com/pulse/us-cyber-trust-mark-empowering-consumers-more-secure-america-zbo4e.

[4] *See*, *e.g.*, Comments of CTA, ET Docket Nos. 21-232 & 21-233 (filed 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 (filed Sept. 20, 2021); Reply Comments of CTA, ET Docket Nos. 21-232 & 21-233 (filed Oct. 18, 2021); Comments of CTA, ET Docket No. 21-232 & 21-233 (filed Apr. 7, 2023); Reply Comments of CTA, ET Docket Nos. 21-232 & 21-233 (filed May 8, 2023).

[5] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 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).

on how to comply and (iv) include a reasonable transition period based on global production cycles. Finally, any new marketing restrictions should avoid imposing significant burdens on trusted manufacturers and the equipment authorization process without commensurate security benefits. CTA elaborates on these recommendations below and welcomes further engagement with the Commission to support effective implementation of the Secure Equipment Act.

II. ANY COVERED LIST IMPLEMENTATION MUST DIRECTLY REFLECT SPECIFIC DETERMINATIONS BY ENUMERATED SOURCES

The FCC should base all Covered List prohibitions solely on specific determinations by Enumerated Sources, as Congress required. CTA and other stakeholders have underscored this imperative in every aspect of this proceeding.[6]

As a general matter, Commission national security prohibitions regarding untrusted suppliers require a specific determination from an Enumerated Source. In passing the Secure Networks Act and Secure Equipment Act, Congress provided clear direction regarding the FCC's role in addressing untrusted suppliers: namely, the FCC must update the Covered List "based solely on" specific determinations from Enumerated Sources and prohibit equipment and services on the Covered List from receiving FCC subsidies or equipment authorization.[7] By acting independently, the Commission would deviate from Congressional direction and supplant the work of other agencies and interagency bodies that Congress or the President have tasked

[6] *See*, *e.g.*, Comments of CTA, ET Docket Nos. 21-232 & 21-233, WC Docket No. 18-89, at 9 (filed June 27, 2025); Petition for Clarification of CTA and the Telecommunications Industry Association (TIA), ET Docket No. 21-232 (filed Dec. 22, 2025) (CTA-TIA Petition for Clarification).

[7] Secure Networks Act § 2(b)-(c). As the *Second Order* explains, 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." *See Second Order* ¶ 5, n.4 (citing National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, § 1709(a)(2) (2024)).

with conducting the large-scale national security reviews necessary to make these determinations.[8] Specifically, the proposals to prohibit the authorization of equipment containing "certain modular transmitters *that are not necessarily produced by entities identified on the Covered List*"[9] or "a range of components, including semiconductors, modular transmitters, GPS and timing modules, and optical transceivers *produced by any person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary*"[10] risk overstepping because the Enumerated Sources have not made a specific determination for either.[11] More, acting outside the Secure Networks Act process would almost certainly put the FCC's rules at odds with actions by Enumerated Sources.

Instead, any prohibitions on components should be directly informed by specific determinations by Enumerated Sources. As CTA and TIA noted in their recent Petition for Clarification on the *Second Order*, specific determinations by Enumerated Sources have provided increasing detail regarding the scope of products covered and appropriate timelines for

[8] For example, Congress established the Federal Acquisition Security Council (FASC) as part of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115–390, 132 Stat. 5173 (2018), to protect federal information communications technology (ICT) systems by recommending exclusion or removal of covered articles that pose too great a risk to the federal enterprise. In addition, President Trump directed the Department of Commerce to review, condition and even potentially unwind transactions involving information and communications technology and services (ICTS) and entities subject to a foreign adversary. Exec. Order No. 13873, 84 Fed. Reg. 22689 (2019). Congress specifically identified both the FASC and the ICTS transaction review process as Enumerated Sources for specific determinations to populate the Covered List. Secure Networks Act § 2(c)(1)-(2).

[9] *Second FNPRM* ¶ 63 (emphasis added).

[10] *Id.* ¶ 64 (emphasis added).

[11] *See*, *e.g.*, H.R. Rep. No. 116-352 (2019) ("The Committee expects that the FCC will monitor these [Enumerated S]ources, *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). This indicates that the FCC has limited discretion.

implementation.[12] The scope and timelines provided in these actions are central to the national security risk determinations by the Enumerated Sources, which reflect careful balancing of national security risk, economic and supply chain impact and other factors, developed in consultation with industry experts. Therefore, to the extent that an Enumerated Source elaborates on the scope and/or timing of a particular prohibition, the Commission's implementation of Covered List prohibitions should mirror that scope and timing.

III. ANY PROHIBITIONS ON COMPONENTS SHOULD BE CAREFULLY TAILORED, INFORMED BY ENUMERATED SOURCES AND ACCOMPANIED BY CLEAR GUIDANCE AND APPROPRIATE TRANSITION PERIODS

Where a specific determination provides little detail regarding the scope of covered products,[13] a targeted, risk-based approach to prohibiting component parts that fall within the equipment and services identified by the specific determination—focused on functionality (rather than broad categories) of components—will best support consistent application of national security restrictions while minimizing negative economic effects. Seeking and incorporating input from the relevant Enumerated Source will enable the Commission to leverage the nation's best investigative resources and intelligence, as envisioned in the Secure Networks Act. Working with industry to develop clear guidance on how to comply with any such prohibition and appropriate transition timelines to reflect global production cycles can best ensure effective implementation of any such prohibition and reduce burdens on trusted manufacturers.

[12] CTA-TIA Petition for Clarification at 4 (citing DHS Binding Operational Directive 17-01 and the Bureau of Industry and Security Final Determination on Kaspersky products as examples of specific determinations with more detail on scope, e.g., than the National Defense Authorization Act for Fiscal Year 2019 (FY19 NDAA) listing of telecommunications equipment and services by Huawei and ZTE).

[13] For example, the FY19 NDAA listings broadly prohibit "telecommunications equipment produced by" Huawei and ZTE, including "telecommunications or video surveillance services provided by such entities or using such equipment." FY19 NDAA, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1918 (2018).

A. A Targeted, Risk-Based and Functionality-Focused Approach Can Help Reduce Significant Challenges of Potential Component Restrictions

The Commission faces a complex challenge in determining whether and how to apply Covered List prohibitions to component parts. This challenge will likely persist as Enumerated Sources make new specific determinations and the technology ecosystem and threat surface evolve. Adopting prohibitions based on broad categories of components could lead to overbroad restrictions that place substantial burdens and costs on trusted manufacturers. For example, prohibiting "authorization of communications equipment that would be covered equipment as a result of its inclusion of *logic-bearing hardware, firmware, or software*" could implicate an array of products that do not pose a national security threat to U.S. networks, while imposing significant expense to manufacturers and the efficiency of the equipment authorization process.[14] Many "logic-bearing" components pose no meaningful security risk because they do not access user information or interact with radio frequency (RF) functions. Without further clarification of these terms, manufacturers, importers and telecommunications certification bodies (TCBs) would struggle to determine which components qualify, leading to inconsistent application across diverse companies with global supply chains. Overly broad or unclear component restrictions could slow product development cycles, increase manufacturing costs, and limit design options. This may place U.S. companies at a competitive disadvantage and hinder innovation and deployment, undermining President Trump's push for American technological dominance.[15]

[14] *Second FNPRM* ¶ 59 (emphasis added).

[15] *See*, *e.g.*, *Winning the Race – America's AI Action Plan*, The White House, at i (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (identifying the "national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance").

Broad component restrictions raise numerous implementation challenges given the complexity of consumer devices, which typically contain modules or subassemblies integrating components from multiple vendors. For example, if a newly restricted component is embedded within a certified module, removing it could require a major redesign of the entire product, involving substantial cost and years to complete. Among numerous questions, the Commission would need to determine and communicate how such a prohibition would impact repair and maintenance of otherwise approved finished products and how owners of such products (particularly small businesses and consumers) would know that a newly covered component is embedded in a particular finished product. The Commission may face instances in which manufacturers do not have records of those component parts for products developed a decade or more ago.[16] With these complications in mind, CTA encourages the Commission to take a targeted, risk-based approach to applying Covered List prohibitions to components and to focus on the function that a particular component performs in the product rather than identifying broad categories.

B. Enlisting Input from Enumerated Sources Can Help the FCC's Implementation Remain Risk-Informed and Aligned with the Rest of the U.S. Government

To support a targeted, risk-based and function-focused analysis of potential component restrictions, the Commission should enlist the help of relevant Enumerated Sources. CTA supports the Commission exploring potential partnership(s) for this purpose as the *Second FNPRM* suggests.[17] Consistent with CTA and TIA's recommendations regarding potential

[16] Any new recordkeeping requirements the Commission considers in this context should be consistent with the FCC's other equipment recordkeeping rules, which generally require 2 years of records. 47 C.F.R. § 2.938(f).

[17] *Second FNPRM* ¶ 65.

restrictions on existing authorizations, any final decision on components should reflect any formal input from Enumerated Sources.[18] Without explicit direction from Congress, an FCC-specific "trusted supplier program" would contradict the Secure Networks Act process (as discussed above) and undermine the procompetitive policies on which the equipment authorization rules are built.[19]

C. Developing Clear Compliance Guidance with Stakeholders Can Significantly Reduce Administrative Burdens and Ensure Consistent Implementation

Should the Commission find it necessary to extend Covered List prohibitions to particular components, the Commission should provide clear guidance so that companies can comply with any new restrictions. Similarly, stakeholder collaboration will be key to developing clear compliance guidance. As with requested clarification regarding the term "produced by," the Commission could accomplish this through a Public Notice issued by the Public Safety and Homeland Security Bureau, roundtable discussions, a multistakeholder committee workstream or some combination of these mechanisms.[20]

D. Appropriate Transition Periods Grounded in Market Realities are Critical to Enable Compliance and Promote Continued U.S. Technology Leadership

Adjusting to any new restrictions on components currently in the supply chain and in product roadmaps will require significant resources in both time and money.[21] As noted above, to the extent that an Enumerated Source details implementation timelines in a specific determination, any application of prohibitions to components based on that determination should

[18] CTA-TIA Petition for Clarification at 6.

[19] *Second FNPRM* ¶ 65.

[20] *See* CTA-TIA Petition for Clarification at 6-7.

[21] *Second FNPRM* ¶ 62 (seeking comment on appropriate transition periods for implementing prohibitions on component parts in order to strike "the appropriate balance between addressing national security concerns in a timely manner and allowing a smooth market transition that minimizes impact on the equipment supply chain").

follow those timelines. Absent clear direction in the specific determination, the Commission should adopt reasonable implementation timelines based on input from relevant stakeholders regarding how long it will take to implement such a change throughout their supply chains. Depending on the scope/nature of such a component prohibition, the Commission may need to consider multiple transition periods because the same component may be incorporated into various finished products with significantly different production cycles. For example, the Commerce Department recognized this need in its Final Rule on connected vehicles, in which it adopted prohibitions on certain software components beginning for model year 2027 and certain hardware components beginning for model year 2030 vehicles.[22]

Absent reasonable transition timelines, new restrictions on components could shock supply chains for finished products across myriad sectors of the U.S. economy. As noted above, many of the technology products consumers enjoy and rely upon today contain complex components and systems built on generations of iterative parts. Manufacturers often make purchasing decisions and design products based on bespoke component parts years in advance of a product rollout. Trusted manufacturers need reasonable transition timelines to implement new component restrictions so that U.S. products remain available and competitive in the global market, and so U.S. innovation continues to dominate the world's technology landscape.

IV. NEW MARKETING RESTRICTIONS SHOULD ONLY IMPOSE BURDENS WITH CORRESPONDING SECURITY BENEFITS

CTA supports the Commission's objective of enhancing security and ensuring compliance via its marketing rules, however, several proposed measures in the *Second FNPRM* could impose substantial burdens without delivering meaningful benefits to aid the

[22] 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.

Commission's implementation of Covered List prohibitions. In particular, CTA urges the Commission to avoid new requirements placing the onus of enforcement on consumers, requiring re-verification of the authorization status of inventory, and introducing expiration dates, time limits or re-certification requirements on equipment authorizations.[23]

Manufacturers and responsible parties comply with extensive labeling, user documentation, and, in some instances, online posting requirements under the existing FCC rules.[24] Adding new consumer-facing obligations risks duplicating many of these requirements without producing meaningful benefits. Relying on consumers to understand the full significance of an FCC ID and to navigate the FCC database for every product they purchase would impose unreasonable burdens with likely little additional benefit. Likewise, many authorized devices do not require FCC IDs or an FCC logo, such as those that are authorized via a Supplier's Declaration of Conformity.[25] Further labeling or point-of-sale disclosure requirements are therefore unlikely to enhance compliance while being difficult to implement consistently across retail channels and potentially confusing consumers who may look for an FCC indicator where none is required. CTA has repeatedly highlighted the consumer benefits of simplified and

[23] For example, the *Second FNPRM* asks whether to "prohibit marketing of RF equipment by entities identified on the Covered List, regardless of the identity of the authorization holder or the production source" (*Second FNPRM* ¶ 86); whether to require an FCC ID number "to be visible on the outside of all packaging" or "on-line retailers to display the FCC ID number in the product listings for all offered RF products that are subject to certification requirements" "so a consumer, in all cases, can easily verify a device's authorization status" (*Id.* ¶ 91); or whether to "explicitly require display of the FCC ID at the online point of sale or at other virtual points of sale" (*Id.* ¶ 93).

[24] *See*, *e.g.*, 47 C.F.R. §§ 2.925, 2.926; *id.* § 2.1074; *id.* § 2.1077; *id.* § 15.19; *id.* § 15.105; *id.* § 20.19; *id.* § 20.21(f)(1).

[25] 47 C.F.R. § 2.1074(b) (providing for the *voluntary* use of the FCC logo as a visual indication that the product complies with the applicable FCC requirements) (emphasis added). *See also* Comments of CTA, ET Docket No. 24-136 (filed Sep. 3, 2024) (discussing the critical role of the Supplier's Declaration of Conformity within the FCC's equipment authorization process).

digitalized labeling and urges the Commission to continue to move towards—not away from—more effective disclosures.[26]

The Commission's existing Part 2 definition of "marketing" already encompasses a broad range of conduct—such as sale or lease, advertising, importation, shipment and distribution for the purpose of selling.[27] Manufacturers, brand owners, importers of record and other responsible parties possess the technical information and authority needed to ensure compliance. Retailers, platforms and other service providers generally do not have access to regulatory authorization or compliance records held by manufacturers.

Requiring importers or distributors to repeatedly re-verify the authorization status of inventory would create substantial logistical and administrative burdens.[28] Large importers often manage thousands of SKUs across multiple warehouses, which would make ongoing verification an intensive task requiring new processes, staff and tracking systems. This could delay product movement through the supply chain, affecting availability and market timing. More, the Commission would be hard-pressed to determine a practical interval for reverification because frequent checks would be unfeasible for high-volume distributors. Given that the vast majority of underlying authorizations rarely change once granted, the cost and effort of repeated verification would far outweigh any compliance benefits.

Adopting expiration dates or time limits on equipment authorizations would also pose significant challenges and would be a sea-change in the Commission's longstanding approach to

[26] *See* Comments of CTA, GN Docket No. 25-133, at 3 (filed Apr. 11, 2025) (CTA Delete Comments); Comments of CTA, WT Docket No. 23-388, at 6-8 (filed Feb. 26, 2024).

[27] 47 C.F.R. § 2.803.

[28] *See Second FNPRM* ¶ 91 (proposing importers or distributors to repeatedly re-verify the authorization status of inventory after intake).

equipment authorization.[29] The consumer technology industry relies heavily on the FCC's established test-once, sell-forever policy to continue innovating new devices rather than look backward.[30] Many long-lifecycle products remain unchanged for years. Industry relies on the Commission's permissive change rules and the staff's related body of guidance to understand when to retest, reauthorize and recertify devices with a new FCC ID.[31] Recertifying devices solely due to an arbitrary time limit would divert engineering resources without improving safety or compliance. Likewise, requiring manufacturers to resubmit full certification applications for products that have not changed would create unnecessary redundancy and substantial cost across both industry and the equipment authorization program. Such a requirement would strain the capacity of TCBs, increasing review times for all applicants and slowing overall market access, amid the Commission's efforts to increase efficiencies, reshore testing and eliminate "bad labs" and TCBs from the system.

Clearer definitions, risk-based approaches and targeted enforcement mechanisms would more effectively address security concerns while avoiding unnecessary disruption to consumers,

[29] *See id.* (seeking comment on whether the FCC should consider implementation of an expiration date or other time limit on equipment authorizations); 47 C.F.R. § 2.906(b) ("Supplier's Declaration of Conformity is applicable to all items subsequently marketed by the manufacturer, importer, or the responsible party that are identical, as defined in § 2.908, to the sample tested and found acceptable by the manufacturer."); 47 C.F.R. § 2.907(b) ("Certification attaches to all units subsequently marketed by the grantee which are identical (see § 2.908) to the sample tested except for permissive changes or other variations authorized by the Commission pursuant to § 2.1043.").

[30] *See Second FNPRM* ¶ 91 (seeking comment on whether the FCC should consider implementation of an expiration date or other time limit on equipment authorizations). In addition, TCBs engage in post-market surveillance to ensure that the devices coming off of manufacturing lines match granted certification. *See id*. ¶ 93 (seeking comment on current equipment authorization compliance monitoring practices); 47 C.F.R. § 2.962(i).

[31] *See* 47 C.F.R. §§ 2.932, 2.1043; FCC, Office of Engineering and Technology (OET), Laboratory Division, KDB 178919 D01 Permissive Change Policy v06 (Oct. 16, 2015); FCC, OET, Laboratory Division, KDB 78919 D02 Permissive Change FAQ v01 (Oct. 16, 2015); KDB Notification 202109-001: Class II Permissive Change for PCB and Part Modification and PAG C2PCPX.

manufacturers and supply chains. In considering updates to the FCC's marketing and enforcement rules, there may be opportunities to align requirements with aspects of the European Union's Radio Equipment Directive to harmonize compliance with allied countries. CTA and other stakeholders have provided recommendations regarding potential enhancements to the equipment authorization marketing and enforcement rules in previous proceedings.[32] We urge the Commission to consider those proposals in any updates to these rules and not let this proceeding or the *Second FNPRM* be the end of the conversation on these important topics, including, for example, liability.

V. CONCLUSION

CTA remains a committed partner and resource for the Commission in the critical, continuous task of implementing the Secure Equipment Act. Ensuring the FCC's implementation remains rooted in specific determinations by Enumerated Sources is consistent with the nation's overall security posture. Any new prohibitions on component parts should (i) reflect a targeted, risk-based approach focused on functionality, (ii) integrate any formal input provided by a relevant Enumerated Source, (iii) be accompanied by clear compliance guidance and (iv) include reasonable transition periods based on global production cycles. To promote effective implementation of these rules and support trusted manufacturers working to comply, any modifications to the FCC's marketing restrictions should only impose burdens with

[32] *See*, *e.g.*, Comments of the Consumer Electronics Association (CEA) n/k/a Consumer Technology Association (CTA), ET Docket No. 15-170 (filed Oct. 9, 2015); CTA Delete Comments; Comments of CTIA, GN Docket No. 25-133, at A-8–A-10 (filed Apr. 11, 2025); Comments of Information Technology Industry Council, GN Docket No. 25-133, at 2-5 (filed Apr. 11, 2025); Comments of Mobile & Wireless Forum, GN Docket No. 25-133, at 6 (filed Apr. 11, 2025).

commensurate security benefits. CTA welcomes further engagement with the Commission on this foundational work.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ J. David Grossman*
J. David Grossman
Vice President, Policy & Regulatory Affairs

/s/ Rachel Nemeth
Rachel Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

January 5, 2026