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
Vice President, Regulatory & Government Affairs

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

September 8, 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

I. INTRODUCTION AND SUMMARY

Consumer Technology Association (CTA)[1] shares the government's commitment to preventing untrusted suppliers from undermining U.S. consumer and national security interests while supporting the entrepreneurship, dynamism and risk-taking that has been so foundational to U.S. leadership in technology.[2] Several proposals in the Third Further Notice of Proposed Rulemaking would levy massive burdens on innovation, reduce consumer choice, increase prices and undermine American technology leadership without creating the meaningful national security benefits that would justify such self-imposed constraints.[3] To avoid these harms, CTA suggests targeted ways to meet the Federal Communications Commission's ("Commission's" or "FCC's") national security goals while ensuring consumers continue to have access to innovative, trusted devices and the United States remains the venue of choice for global business.

[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 17 million American jobs. CTA owns and produces CES®—the most powerful tech event in the world.
[2] *See generally* Gary Shapiro, *Pivot or Die: How Leaders Thrive When Everything Changes* (2024).
[3] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Third Report and Order and Third Further Notice of Proposed Rulemaking, ET Docket No. 21-232, FCC 26-50 (rel. July 23, 2026) ("*Third Order*" and "*Third FNPRM*").

Changes to these equipment authorization rules that may seem minor to some could have catastrophic consequences for how innovators bring modern technologies to consumers. For example, the Commission asks whether to narrow the trade show exclusions that permit the importation and demonstration of limited numbers of unauthorized devices.[4] This exemption is a foundational facilitator of the modern consumer technology market: Every year, thousands of startups and established companies bring cutting-edge innovation to CES and 100,000 business executives walk the exhibit halls to understand how consumer technology is progressing.[5] Although most devices demonstrated at CES are FCC equipment authorized, many are still in development or are intended for international markets. The current rules allow importation and demonstration of these different types of devices, and America benefits. CES alone supports approximately 1746 jobs, equating to $92.5 million in salaries and wages and $396 million in "economic impact." Businesses conduct billions more in deals while demonstrating U.S. technology leadership to the world. CTA looks forward to welcoming 150,000 attendees at CES 2027 to experience how new technology advancements are delivering benefits across nearly every sector of the U.S. economy and enhancing Americans' daily lives. CES and similar stops (literal and metaphorical) on the path to commercialization are essential to the competitive, dynamic consumer technology industry.

The FCC's equipment marketing, importation, operation and authorization rules support innovation by enabling iterative design, product testing and pre-sales marketing that attracts capital and facilitates other go-to-market activities. The current exceptions for unauthorized and

[4] *Third FNPRM* ¶ 166.

[5] CES 2026 featured more than 4100 exhibitors, including some 1200 startups, highlighting technology that is solving some of the world's greatest challenges. The event showcased cutting edge innovations in accessibility, AI, content and entertainment, digital health, energy, enterprise, mobility, robotics, smart glasses and wearables, smart home, startups, and more. *See* Press Release, CTA, *CES 2026: The Future is Here* (Jan. 9, 2026), https://www.ces.tech/press-releases/ces-2026-the-future-is-here.

pre-authorized devices, along with flexibility to pursue varied design and manufacturing relationships, are not loopholes; they are critical enablers of the dynamic consumer technology marketplace. The present equipment authorization regime ensures that consumers have a wide variety of affordable technology products from a robust base of trusted suppliers from like-minded countries.[6]

The consumer technology industry remains committed to national security and to the integrity of the device ecosystem. CTA worked closely with the Commission to implement the Secure Networks Act and the Secure Equipment Act and championed supply chain risk management efforts—like the FCC IoT Cybersecurity Labeling Program—that can complement these efforts, enhancing security at a global scale.[7]

Prohibitions on FCC equipment authorization are one tool Congress provided under specific, extremely high-risk circumstances, among a multifaceted array of levers and partnership opportunities available to enhance supply chain security and ensure trusted suppliers

[6] *See* Gary Shapiro, *Made in America needs global partners*, Newsweek (May 2, 2026), https://www.newsweek.com/made-in-america-needs-global-partners-opinion-11893025 ("Resilience does not mean pulling everything back within U.S. borders. Real resilience comes from diversifying. That means reshoring where it makes sense, near shoring where it's efficient, 'friend shoring' with trusted allies and trading partners and recognizing that trade with countries like China will continue to be part of the economic mix").

[7] *See* 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. §§ 1601-09) (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); U.S. Cyber Trust Mark, FCC, https://www.fcc.gov/CyberTrustMark (updated Aug. 11, 2026). CTA and partners across the consumer technology ecosystem continue to work with the Commission toward a voluntary labeling program that will incentivize continuously evolving cybersecurity and supply chain risk management across the globe. *See Cyber Labeling for Connected Devices*, CTA, https://www.cta.tech/cyber-labeling-for-connected-devices (last visited Sept. 3, 2026).

compete on an even playing field in the global market. FCC equipment authorization has never and should never be repurposed as a tool for widespread economic engineering.[8]

To strengthen the equipment authorization framework and national security, CTA recommends a risk-based, appropriately tailored, clear and administrable approach—one that targets genuine security threats while preserving timely access to innovative technologies and minimizing unnecessary burdens on responsible manufacturers, importers and retail partners. As an overarching matter, four key principles should guide the Commission's rulemaking:

- Prioritize the efficiency of the FCC's equipment authorization process to ensure American consumers and businesses maintain access and choice in market-leading technologies and to promote U.S. technology leadership abroad;
- Ensure Covered List rules and implementation directly align to statutory intent, including specific determinations by Enumerated Sources in the Secure Networks Act;
- Preserve the flexibility needed to bring innovation to market throughout every stage of design, development and deployment—including critical protections for trade shows like CES; and
- Keep enforcement focused on bad actors rather than imposing marketplace-wide burdens that harm good-faith actors without commensurate security benefit.[9]

CTA supports the *Third FNPRM*'s proposals to bifurcate the Covered List, allow changes to covered equipment to support continued functionality and a transition to more trusted equipment and the Commission's efforts to provide additional clarity—but is concerned that other proposals would merely impose significant burdens on responsible manufacturers. The

[8] Using "national security," which is an exemption to the President's deregulatory Executive Orders, as a pretext to indiscriminately regulate technology would frustrate the President's directive to "deconstruct[] … the overbearing and burdensome administrative state" and the types of "regulations that are based on unlawful delegations of legislative power." *Executive Order 14219 of February 19, 2025, Ensuring Lawful Governance and Implementing the President's "Department of Government Efficiency" Deregulatory Initiative*, 36 Fed. Reg. 10583 (Feb. 25, 2025); *see also Executive Order 14192 of January 31, 2025, Unleashing Prosperity Through Deregulation*, 24 Fed. Reg. 9065 (Feb. 6, 2025).

[9] With over two hundred questions, proposals and tentative conclusions, these comments cannot address every CTA member priority, and CTA offers these guiding lodestars for both those issues addressed below and those that CTA will not be able to address during the rushed comment cycle.

FCC can advance security objectives while protecting proprietary information, minimizing unnecessary administrative burdens, and preserving the competitiveness of U.S. manufacturers in the global marketplace.

Several of the proposals in the *Third FNPRM* would likely have widespread and deleterious consequences for the entire technology industry.[10] Certain of these proposals would create tremendous implementation and compliance challenges: disrupting the FCC's existing equipment authorization processes, slowing or deterring innovation, and potentially making it more difficult for consumers to obtain and use the devices they rely on. Re-imposing regulations after implementing successful regulatory reform would undermine this Administration's goals of reducing and deleting regulatory burdens. Introducing new steps to market authorized devices will add costs that will be passed along to consumers without increasing security, such as those that impose additional regulations on retailers, clutter boxes and point-of-sale displays and require recertifying established devices. The new steps would also likely generate consumer confusion rather than assurance.

Additional disclosure, reporting and certification requirements will be costly and administratively burdensome without meaningfully improving either economic or national security. The FCC has successfully identified fraud with the information in its own records and through third-party security researchers. Increasing compliance burdens on compliant companies is unlikely to deter any bad actors that have been undeterred by the current rules.

CTA is committed to device security and urges the FCC to fully consider the practical and legal issues implicated by broad changes to the design and development of radiofrequency

[10] The proposals in the *Third FNPRM* reach nearly every stage of the equipment-authorization process—from sharp cuts to pre-authorization importation and testing, to new restrictions on marketing, to mandatory hardware and software bills of materials, to an expansive reading of "produced by," to re-certification and authorization-expiration requirements—and CTA addresses these in turn below.

(RF) devices proposed in the *Third FNPRM* beyond those envisioned by Congress. The FCC has drastically underestimated the costs and administrative burdens these actions would incur, both to industry and to the government. Imposing additional regulations and requirements will increase direct costs such as diverting staff resources from innovation to government compliance. The Commission will have to commit significant resources to intake and protect new, highly sensitive information. Several of the reporting proposals would require significantly new information with applications in the aging Equipment Authorization System database.[11] For example, requiring registrations related to devices approved via Supplier's Declaration of Conformity (SDoC) would likely require a new web portal. Limiting standard marketing, testing, branding activities will also cause massive opportunity costs in the form of delayed product launches and chilled innovation.

The American consumer technology industry thrives on clear rules and predictability as to when and how those requirements change. Should the Commission reimagine the general equipment authorization program, industry must have time—at least three years—to adjust to any of the dozens of new regulations the *Third FNPRM* proposes while, at the same time, the Commission updates its databases and websites to accommodate its new regulations.

II. DYNAMIC INNOVATION RELIES ON THE FCC'S FLEXIBLE, STREAMLINED PRE-AUTHORIZATION PROCESS

The Commission's rules expressly permit numerous activities that facilitate the development of secure devices that ultimately go to market in the United States and globally from American companies. Rather than being loopholes, Rules 2.803 and 2.805 and subpart K[12]

[11] *Third FNPRM* ¶ 216; *see also id.* ¶ 142 (proposing HBOM and SBOM submissions and a 30-day update requirement).
[12] *See* 47 C.F.R. §§ 2.803, 2.805; *id*. pt. 2, subpart K.

are critical *milestones* on the road from hand-built prototype to billion-dollar consumer product and from buddies in a garage to public SEC filings.

Certain proposals in the *Third FNPRM* would roll back the 2021 and 2017 regulatory reforms,[13] along with longstanding flexibility that allows innovators to conduct research, develop and test devices; gauge consumer interest; and prepare for product launches. Startups and established companies have relied on these flexibilities to move new technologies from concept to market to consumers. In 2021, when acting on CTA's petition,[14] the FCC anticipated that its reforms would "further the communications sector's ability to drive innovation that will advance America's global competitiveness and promote economic growth,"[15] and this has happened.

A. Limited Importation of Unauthorized Devices Empowers Research, Development and Sales without Creating National Security Concerns

The current marketing exceptions and importation conditions strike an appropriate balance between ensuring nearly all imported and marketed devices have equipment authorization and supporting a lawful and efficient path to importation for the beneficial and secure uses of unauthorized RF equipment.

Foreclosing or sharply curtailing the importation of unauthorized RF devices, as proposed, would ripple across the entire development cycle.[16] It would limit research and development, slow product refinement and competitive analysis, complicate model-specific advertising and launch campaigns, and drive the global device deals now transacted on U.S. soil

[13] *Allowing Earlier Equipment Marketing and Importation Opportunities*, Report and Order, 36 FCC Rcd 10544 (2021) (*2021 Equipment Authorization Order*); *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, First Report and Order, 32 FCC Rcd 8746 (2017) (*2017 Equipment Authorization Order*).
[14] Petition of Consumer Technology Association to Expand Marketing Opportunities for Innovative Technologies, RM-11857 (June 2, 2020).
[15] 2021 Equipment Authorization Order ¶ 1.
[16] *Third FNPRM* ¶¶ 159-67.

to other markets, even for covered equipment. Cutting the units available for pre-authorization importation—by as much as a factor of 100x in some cases—is particularly concerning, because companies need enough prototypes to carry a device through its full engineering and testing cycle, including the many revisions that precede formal testing.[17] Innovators often refine products on American soil before settling on a final configuration for authorization. They routinely import test units to gauge customer acceptability and interoperability, to demonstrate devices to investors and retail buyers, to develop marketing strategies with hands-on hardware, benchmark against other devices in the global market and research security issues. A 40-unit cap cannot accommodate those overlapping needs. Restricting the importation of RF devices in this way would reduce global device sales and marketing deals done in the United States and perversely incent cruder devices entering the marketplace, among other adverse consequences.

The FCC should maintain these importation conditions because the existing quantity allowances are essential for engineering validation, regulatory testing, customer and interoperability testing, and product-launch preparation. The rules recognize the need for pre-authorization activities by permitting as many as 400 units for a trade-show display[18] and 12,000 units for pre-sale staging.[19] Reducing those amounts would delay U.S. commercialization without any national-security benefit. The proposed cap of 40 units for engineering and testing that precede the trade-show display and pre-sale staging phases of the equipment authorization process would hamstring research and development and likely reduce the number of devices able to be introduced for display at trade shows or that need pre-sale staging.

[17] Today, manufacturers and others may import 4000 or fewer units for testing without an FCC-issued equipment authorization, provided the devices are not marketed or sold. 47 C.F.R. § 2.1204(a)(3). The *Third FNPRM* proposes a reduction from 4000 units to 40 units. *Third FNPRM* ¶ 161.
[18] *See 2017 Equipment Authorization Order* ¶ 61; 47 C.F.R. § 2.1204(a)(4)(i).
[19] *See 2021 Equipment Authorization Order* ¶ 13; 47 C.F.R. § 2.1204(a)(11).

This runs contrary to the Commission's decision under Chairman Pai to expand the number of units available for importation at trade shows to reflect the importance of these events to the consumer technology market and to reduce administrative burdens associated with constantly applying for waivers of the importation caps.[20] Maintaining these numbers today will not raise risks to national security.[21] Indeed, the FCC's existing guardrails ensure the defined small quantities of excepted devices are consistently accounted for and never put in a position to support critical (or even commercial/consumer) infrastructure. At the same time, such an impediment to fundamental engineering and testing decreases the potential for American innovation and leadership.

The FCC should affirm the existing exemptions for the importation and use of covered equipment, including equipment produced by entities on the Covered List for research, development, and testing purposes.[22] Allowing the importation of such equipment for these limited purposes will further innovation without posing risk to national security, as the equipment will be confined to specific environments and monitored, rather than in the hands of end users. The Commission should permit this narrow category of uses of "covered" equipment to enter the U.S. at the scale needed to support U.S. innovation and leadership. Even products from producer/provider-based Covered Listings provide value to the innovation ecosystem in the context of trade show and other exemptions, where importing a *de minimis* quantity of devices not ultimately eligible for Commission authorization allows experts to explore, understand, and effectively compete in the international market.

[20] *2017 Equipment Authorization Order* ¶ 61.
[21] *Cf. Third FNPRM* ¶ 161 (seeking comment on the appropriate quantity of devices for testing and evaluation and inviting evidence on whether a greater number is needed).
[22] *See id.* ¶ 160; 47 C.F.R. § 2.1204(a).

Should the Commission decide to reduce the available importation conditions for RF devices, including the number of units permitted per condition, the final rules should clearly preserve exceptions for: (i) engineering and product development; (ii) laboratory and regulatory testing; (iii) customer evaluation and demonstration; (iv) trade shows and exhibitions; (v) repair and servicing; (vi) re-export only; (vii) personal use; (viii) pre-sales activities and (ix) U.S. government activities.[23] Additionally, the FCC should continue to allow the Chief of the Office of Engineering and Technology to provide written approval for the importation of a greater number of a certain model of covered equipment.[24]

B. Marketing Opportunities for Unauthorized Equipment Generate Necessary Capital and Investment

The Commission expanded pre-authorization marketing opportunities in the last decade to increase American competitiveness in the consumer technology market here and abroad. The Commission explained in 2021:

> As product development cycles have accelerated, new marketplace models and assessment tools have emerged that rely on individual interest to fund products, optimize production, and match imports to anticipated sales. The [new] rules … will allow manufacturers to better use these tools to quickly deploy new technologies and devices to consumers while ensuring that communications equipment subject to equipment authorization continues to meet our stringent program requirements.[25]

Maintaining the United States as the place-of-choice for global business benefits American economic and national security.[26]

---

[23] *See* 47 C.F.R. § 2.1204(a)(1)-(11); *Third FNPRM* ¶¶ 162-66.
[24] *Third FNPRM* ¶ 161. If the Commission deems additional oversight necessary, the FCC can require parties to maintain proof that the devices are either exported out of the U.S. after a certain period of time or have been destroyed rather than released into the flow of commerce.
[25] *2021 Equipment Authorization Order* ¶ 1.
[26] *Third FNPRM* ¶ 170 (proposing to restrict the marketing of covered equipment before authorization).

The *Third FNPRM* correctly identifies that significant marketing resources may be "wasted" where "equipment is later determined to be covered equipment and consequently prohibited," but it prescribes the wrong medicine: to severely limit marketing.[27] The Commission's own analysis supports a more targeted fix. The *Third FNPRM* concedes that the current rule "promotes innovation" and that its proposed restriction would introduce "delays in stakeholders' marketing plans."[28] Timely, transparent notice of Covered List additions—not a broad marketing ban—is the least-burdensome way to "prevent wasted marketing efforts," and it preserves crucial pre-market activity of pre-authorization devices. This approach would also be consistent with the Administrative Procedure Act, the Secure Networks Act and the Secure Equipment Act by providing additional notice and process related to Covered List additions to better alert industry to national security risks and preserve the benefits of the current rules.[29]

C. Operating Devices Before Formal Equipment Authorization Provides Important Product Feedback and Sales Opportunities

Companies operate devices before authorization for concrete, constructive reasons, such as confirming customer acceptability, validating security and interoperability and verifying compliance with the Commission's own rules. Demonstrating a device at a trade show or to prospective buyers is often what generates the early reviews, consumer interest and investment that carry a product to market. Because both security and interoperability must be validated before scale manufacturing begins, operating a device for testing is not a loophole. For covered equipment in particular, security testing directly serves national security and resilience.

[27] *Id*. ¶ 171.
[28] *Id*. ¶¶ 169, 171.
[29] *Id*. ¶ 171; *see also id*. ¶ 169 (acknowledging that the current pre-authorization marketing rule "promotes innovation by increasing the speed with which a company can bring a new device to market").

The existing Rule 2.805 exception also functions as a safety valve when authorization is delayed (such as during a government shutdown) so that launches and trade show demonstrations can proceed.[30] If the government identifies bad actors exploiting these flexibilities, it has ample tools to respond through targeted Department of Justice, Federal Bureau of Investigation, and FCC enforcement, without erecting market-wide barriers that fall hardest on good-faith participants.

Eliminating user testing prior to authorization may also lead to less accessible devices, harming consumers and preventing companies from satisfying other Commission requirements.[31] The Commission's accessibility rules contemplate and require user testing.[32] User testing is a key aspect of accessibility-by-design, which is almost always more effective and economically efficient than retrofitting designs. Recently adopted rules, based on an advocate-industry proposal, expressly require user testing of covered apparatus.[33]

In addition, CTA asks the FCC to clarify that temporary testing, evaluation, or demonstration does not constitute unauthorized marketing or commercial operation where the equipment is not being offered for sale or lease in the United States.

[30] The narrow marketing exceptions in Rule 2.803 provide a similar safety valve for marketing, such as for large product launches. *See* 47 C.F.R. § 2.803.
[31] *Third FNPRM* ¶ 196 (proposing to revise 47 C.F.R. § 2.805 and questioning whether developmental, design, and pre-production evaluation provisions are warranted for covered equipment).
[32] *See* 47 C.F.R. § 14.20(b)(1)-(2) (requiring manufacturers of advanced communications services equipment to consider accessibility performance objectives at the design stage "as early as possible" and to "identify barriers to accessibility and usability" as part of product evaluation); *id.* § 14.20(a)(3).
[33] The Commission's recently adopted display-settings accessibility rules expressly require user testing. *Accessibility of User Interfaces, and Video Programming Guides and Menus*, Third Report and Order, 39 FCC Rcd 8292 (2024).

III. ADJUSTING THE COVERED LIST RULES TO THE NEW PRODUCTION LOCATION-BASED CATEGORIES IS NECESSARY FOR IMPLEMENTATION

Over the last eight months, the FCC's Covered List has shifted drastically to accommodate new production location-based prohibitions.[34] Unlike the producer/provider-based prohibitions on which the FCC's Covered List rules were designed and implemented, these new prohibitions: (i) are based on a national security determination from an unidentified "Executive Branch interagency body with appropriate national security expertise" that provides no notice to affected parties before prohibitions become public and effective; (ii) bar "all foreign-manufactured" categories of products (rather than specific products from named entities, specific countries, or specific facilities demonstrated to have posed a national security threat); and (iii) are subject to frequent change after becoming effective as individual entities—or even classes of products within the banned category—achieve Conditional Approvals from the Department of War (DOW) or the Department of Homeland Security (DHS).[35] The *Third Order* aptly

[34] *See, e.g.*, *FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List*, Public Notice, ET Docket No. 21-232 *et al.*, DA 26-278 (PSHSB rel. Mar. 23, 2026); *Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List*, Public Notice, 40 FCC Rcd 10215 (PSHSB 2025); *FCC's Public Safety and Homeland Security Bureau Announces Addition of Foreign-Produced Power Inverters and Advanced Robotic Devices to FCC Covered List*, Public Notice, ET Docket No. 21-232 et al., DA 26-786 (PSHSB rel. July 28, 2026) (*First Power Inverters PN*).

[35] *See, e.g.*, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, 35 FCC Rcd 14284, 14312 ¶ 61 (2020); *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered Routers*, Public Notice, ET Docket No. 21-232, DA 26-286 (PSHSB rel. Mar. 23, 2026); *FCC's Public Safety and Homeland Security Bureau Announces That "Toy Drones" and "Toy Drones That Contain Foreign-Produced Components" Are Removed from the FCC Covered List*, Public Notice, ET Docket No. 21-232 et al., DA 26-588 (PSHSB rel. June 15, 2026); *Following New National Security Determination, FCC Announces Modification of Power Inverters Entry on the Covered List*, Public Notice, ET Docket No. 21-232 *et al.*, DA 26-870 (PSHSB rel. Aug. 20, 2026) (*Second Power Inverters PN*). The FCC provides interpretation of the evolving production-location-based Covered List entries via three separate FAQ pages.

recognized the distinct nature of this category of Covered List updates,[36] and CTA encourages the FCC to distinguish between these categories in its rules going forward.

Specifically, CTA appreciates the Commission's proposal to bifurcate the Covered List and related rules, recognizing that the new "production location-based" listings are far afield from those designed to address specific national security risks from named entities.[37] The "production location-based" listings reflect materially different national security risks and priorities, pose distinct implementation challenges and therefore merit separate treatment under the FCC's rules. These production location-based Covered List updates present unique challenges to implementation as companies (even those without products directly subject to the prohibition) scramble to respond to an unpredictable, evolving, ephemeral, and often imprecise set of supply chain rules.

CTA also supports additional flexibility for certain software and firmware updates as well as hardware swaps.[38] As the Commission has recognized throughout its implementation of the first production location-based Covered List updates, this flexibility is critical to ensuring the ongoing viability of previously authorized equipment consistent with FCC rules. Codifying its policies rather than taking a waiver approach will provide a more level playing field and predictability going forward and as the Covered List continues to evolve.

The Commission can further help by providing additional clarity regarding which products and activities are covered by the evolving Covered List. For example, law-abiding companies puzzle over the contours of the production-location based classifications and struggle with the broadening application of entity-based listings beyond the finished devices listed on the

[36] *See Third Order* ¶ 37 (emphasizing that the prohibitions on logic-bearing hardware components apply only to producer/provider-based determinations).
[37] *Third FNPRM* ¶ 129.
[38] *Id.* ¶¶ 187-95.

Covered List. Any additional clarification must remain rooted in underlying national security determinations and avoid damaging beneficial commercial practices. Specifically, the Commission should:

- Ensure beneficial commercial relationships are not captured by the definition of "produced by" and avoid adopting compliance requirements that would unnecessarily overburden good faith equipment authorization participants.
- Avoid unilaterally applying Covered List prohibitions to software and other components without specific direction to do so by an Enumerated Source.

With respect to authorizing equipment, any changes should generate security benefits that outweigh administrative costs and burdens on the design, development and deployment process that will hinder innovation, technology access, U.S. leadership and American competitiveness.

A. Bifurcating the Covered List Helps Account for Fundamentally Different National Security Concerns and Implications Between Entity-Specific Producer/Provider Listings and Broader Production Location Bans

Production location-based Covered List updates respond to a different national security threat than the producer/provider-based determinations on which the Covered List was founded. While producer/provider-based bans target the unique ability and likelihood of a foreign adversary to exploit a particular company's role in technology supply chains (*e.g.*, to exfiltrate sensitive data or disrupt critical infrastructure), new production location-based Covered List updates identify a general risk of American dependence on foreign production and focus on generating a domestic manufacturing base.[39] They also fail to account for companies' legitimate market incentives to secure their facilities to protect ongoing user trust and guard against exposure of valuable trade secrets and intellectual property that would undercut competitiveness and profits. The producer/provider-based category presents a challenging, but identifiable group

[39] *See Third Order* ¶¶ 9-10 (describing the new production location-based determinations and distinguishing them from producer/provider-based determinations); *Third FNPRM* ¶ 129.

of entities and products that trusted suppliers can work to address and avoid, while the production location-based category is inherently imprecise and subject to continuous change as ownership, staff and the technology ecosystem evolves over time.

These categories also pose distinct implementation challenges. So far, production location-based listings have imposed sector-wide prohibitions for all non-U.S. manufacturing without prior public notice. In addition, the scope of the production location-based bans changes on a near-weekly basis in response to Conditional Approvals and other efforts to conform the Covered List entries to the underlying national security determinations (*e.g.*, subsequent national determinations and intermittent updates to Frequently Asked Questions lists).[40] The extent to which a particular product is covered or will remain covered is unpredictable, exacerbating an already challenging environment for supply chain procurement planning.

As the Commission has heard repeatedly over the last year, rapid growth in new technologies (like robotics, connected vehicles and drones) and underlying infrastructure (like data centers, satellite systems and industrial automation) is driving unprecedented demand for key electronics components.[41] To triage this demand, component manufacturers are prioritizing high-volume, long-term builds rather than preparing broad flexibility for varied immediate needs across the market. This heavily favors buyers that can plan component needs far in advance

[40] *See generally List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, FCC, https://www.fcc.gov/supplychain/coveredlist (last updated Aug. 28, 2026).

[41] *See, e.g.*, AT&T Services Petition for Expedited Waiver of Sections 2.932(b) and 2.1043(b) of the Commission's Rules to Permit Targeted Class I and Class II Permissive Hardware Changes to Covered Routers, ET Docket No. 21-232, at 3 (May 11, 2026) (discussing the global, chronic shortage of certain memory components driven by large-scale AI deployments); NCTA Petition for Expedited Waiver, ET Docket No. 21-232, at 8-9 (June 2, 2026) (discussing persistent industry-wide substrate shortages causing delays and supply chain constraints triggered by increased demand and material shortages); *2026 Electronic Component Shortage Update: What Buyers Should Watch*, Melson Components, https://www.melsonchip.com/2026/05/21/2026-electronic-component-shortage-update-what-buyers-should-watch (last visited Sept. 3, 2026).

rather than those responding to component end-of-life shortages or regulatory shifts with short-term effective dates.[42] In addition, the rising costs of critical materials like copper, silver, gold, PCB laminate and copper foil are driving up prices throughout the technology stack.[43] Together, these supply chain dynamics place extraordinary challenges on consumer technology suppliers. While new bans on specifically-named entities present significant challenges in such an environment, prohibitions on "all foreign" categories of products—intended to be rescoped after their effective dates—make supply chain planning nearly impossible.

CTA commends the Commission's proposal to bifurcate the Covered List to distinguish between "producer/provider-based" and "production location-based" categories.[44] Although the Commission may have limited influence over the underlying national security determinations themselves, CTA appreciates that the Commission has aptly recognized that these two distinct categories merit separate treatment under the FCC's implementation rules. As the Commission recognized in its decision to only apply prohibitions on "logic-bearing hardware components" to producer/provider-based determinations, certain rules are not appropriate for production-location-based categories.[45] CTA encourages the FCC to continue limiting implementation of production location-based bans to the final product and avoid imposing component-level bans, third-party reporting obligations and other requirements that are unnecessary to fulfill the Commission's statutory responsibilities.[46]

---

[42] *See* Ashley Papa, *Why Passive Components Are Emerging as a 2026 Supply Risk*, Fusion Worldwide (Jan. 5, 2026), https://www.fusionww.com/insights/why-passive-components-are-emerging-as-a-2026-supply-riskhttps://www.fusionww.com/insights/why-passive-components-are-emerging-as-a-2026-supply-risk.

[43] *Id.*

[44] *Third FNPRM* ¶ 129 (proposing to bifurcate the Covered List into producer/provider-based and production location-based categories).

[45] *See Third Order* ¶ 37 (limiting the logic-bearing-hardware-component prohibition to producer/provider-based determinations).

[46] *Third FNPRM* ¶ 155.

B. Allowing Certain Permissive Changes Will Avoid De Facto, Retroactive Bans and Support Equitable, Predictable Application of the FCC's Rules

CTA and its members appreciate the Commission's recognition that, to maintain the viability of previously authorized products, suppliers must be able to continue to provide software updates and patches and make certain hardware swaps within a challenging global supply chain environment.[47] Allowing additional permissive changes for covered equipment will ensure the continued functionality and availability of devices while supply chains react to swift and blunt categorical supply chain shocks. Specifically, CTA agrees that the following should be permitted for covered equipment going forward: (i) software and firmware updates that mitigate harm to consumers; and (ii) hardware modifications that do not introduce new security risks or enhance a device's capabilities.[48]

All previously approved products on the Covered List should have access to the new permissive change provisions. The FCC has already asserted authority to limit previously authorized devices in producer/provider-based categories, so there is no need to exclude those from a permissive change because the Commission can easily curtail their authorizations.[49] For the producer/provider-based listings that the FCC has *not* limited, there is the same public interest in ensuring those products can continue to receive patches/updates and make hardware swaps subject to the criteria laid out in the *Third FNPRM*. In other words, if the Commission finds that it must immediately eliminate producer/provider listings, then it should do so through

[47] *Id.* ¶¶ 187-95.
[48] *See generally id*. ¶ 193.
[49] *See Public Safety and Homeland Security Bureau and Office of Engineering and Technology Prohibit the Importation and Marketing of Previously Authorized Covered Communications Equipment Added to the Covered List in 2024 or Earlier*, Public Notice, PS Docket No. 26-72, DA 26-635 (PSHSB/OET rel. June 26, 2026) (prohibiting the continued importation and marketing of certain previously authorized covered equipment added to the Covered List in 2024 or earlier).

the existing limitation/revocation process. If not, then the authorization holders need these permissive change waivers to continue to use and support previously authorized devices.[50]

CTA members further ask the Commission to confirm that: (i) existing Class I permissive changes remain available where a component substitution does not degrade electromagnetic compatibility/RF compliance or require a change to the grant; (ii) existing Class II permissive changes remain available where a modification may affect RF characteristics but can be evaluated, tested, and documented through the existing process without a new FCC ID or new authorization; (iii) software and firmware updates that maintain usability, correct defects, improve security, or address vulnerabilities remain permitted where they do not expand the device's RF capability or change its intended use; and (iv) hardware substitutions for discontinued, end-of-life, or constrained components remain eligible for permissive-change treatment where the modified device remains electrically equivalent and continues to meet applicable FCC limits.

Preserving flexibility is essential not only for commercial supply-chain resilience but also for cybersecurity, repairability and continued support of products in the field. The recent permissive-change waivers—which allow security and firmware updates and like-for-like hardware swaps for covered equipment—confirm that this ordinary lifecycle maintenance can and should proceed without triggering full re-certification.[51] Consistent with this, the Commission should avoid rules that would force previously authorized products into full re-certification (and costly, time-consuming Conditional Approval applications) solely because of

[50] The *Third FNPRM* proposes that "the modified device is equipment in a producer/provider-based Covered List entry, rather than a production location-based Covered List entry." *Third FNPRM* ¶ 193. To the extent the Commission limits permissive changes to a category of covered equipment, CTA requests that the categorical, production location-based entries qualify for permissive changes.
[51] *See id.* nn.31-33.

ordinary lifecycle maintenance, supply-chain substitution, cybersecurity patching or firmware maintenance.

C. Clear Definitions Will Support Implementation of UAS and Router Covered List Prohibitions

A consistent standard for "produced in a foreign country" is appropriate so that the meaning of this phrase does not vary from Covered List category to category.[52] A "domestic end product" standard was adopted in the recent robotic/inverter decision and is likely more tailored to the national security determination than the Federal Trade Commission's (FTC's) Made in the United States framework.[53]

The domestic end product and the FTC's Made in the United States standards serve materially different purposes. The FTC's "Made in the United States" framework is a consumer-protection and marketing standard that governs when a product may be advertised as American-made, and it generally requires final assembly, significant processing and that virtually all components originate in the United States. The "domestic end product" standard, by contrast, derives from federal procurement law, asking whether a product was manufactured in the United States and satisfies a defined domestic-content threshold—an inquiry focused on supply-chain provenance rather than advertising claims. Because the production location-based determinations are concerned with where a product and its critical inputs are manufactured, the "domestic end product" standard is more closely tailored to the underlying national security determination than the marketing-oriented "Made in USA" framework. CTA also urges the Commission to consider

[52] *See id.* ¶ 198 (proposing to interpret equipment as "produced in a foreign country" if it either fails to qualify as a "domestic end product" under federal procurement rules or was designed or developed in a foreign country).
[53] *See id.* ¶¶ 197-207 (seeking comment on how to define "produced in a foreign country," including whether to adopt a broader standard based on the FTC's "Made in the United States" framework, which generally requires final assembly, significant processing, and virtually all components to originate in the United States, or a narrower rule based on trade-law country-of-origin principles).

eliminating the "designed or developed" language from the definition: treating a device built in the United States as "foreign" because some design or software work occurred abroad would penalize domestic assembly and onshoring.

IV. ADDITIONAL CLARITY GROUNDED IN CONGRESSIONAL INTENT WILL REDUCE BURDENS ON STAKEHOLDERS AND ENSURE A CONSISTENT NATIONAL SECURITY POSTURE

A. The Commission Should Adopt a Clear Definition of "Produced By" While Preserving Productive Commercial "White Labeling" Arrangements

CTA understands the Commission's concern regarding the authorization of privately labeled, rebranded or relabeled (white labeled) covered equipment and appreciates the Commission's efforts to clarify the definition of "produced by" to support clear and consistent compliance.[54] CTA supports the Commission's proposal to interpret a device as "produced by" an entity if that entity "exercises substantial responsibility for or control over any major stage of the process by which the device comes into existence, including the design, manufacturing, assembly or development of the device" and noting that "a device may be 'produced by' more than one entity."[55] However, certain terms in this definition and the scope of responsibilities throughout the supply chain requires additional guidance.

The terms "substantial responsibility for," "control over" and "major stage" leave ambiguity regarding some activities that are common within the product development process. For example, a company that uses joint development manufacturing and global R&D teams may not be able to determine where "substantial responsibility" begins and ends. A trusted supplier may have little insight into or control over whether a third-party entity in a high-risk jurisdiction contributes a significant portion of code or a specific hardware module.

[54] *Id*. ¶ 130.
[55] *Id*. ¶ 134 (proposing to define "produced by").

Accordingly, the Commission should clarify that an equipment authorization applicant's diligence obligation extends only to its immediate suppliers and, at most, its second-tier suppliers, and that "substantial responsibility for or control over" a major stage of production reaches only those entities whose contribution exceeds a meaningful threshold of the finished device's value or functionality. A trusted supplier should not be deemed to have "produced" a device based on attenuated, sub-tier contributions that it cannot reasonably identify or control.

The definition should also clarify that suppliers are only responsible for primary inputs into their products. In other words, an equipment authorization applicant must know who sold the part, but cannot also be expected to audit who designed the logic inside the part and where the firmware was written.[56] To require otherwise would be significantly costly and burdensome and require a level of transparency that sub-tier suppliers consider proprietary and are unwilling to share.

The Commission should also clarify that this definition does not include beneficial activities that enable the use of international standards and specialization in the supplier market. For example, cellular standards bodies could be exercising "substantial control over" the design or development of a cellular module by requiring compliance for interoperability; a satellite operator could be exercising "substantial control over" a terminal design because they require the terminal to meet antenna, electrical, waveform, data content and performance requirements; or "Company X" could be exercising "substantial control over" the design or development of third-party products—none of which enables a foreign adversary to exploit a device's presence in U.S.

[56] To the extent the Commission determines it requires some extra assurance for national security reasons, applicants can retain an additional attestation from primary suppliers that certify that these activities were not performed by a Covered List entity. The Commission could then request the retained attestation during an investigation. The Commission should not require Responsible Parties to force the disclosure of sensitive business information regarding the identity of their own suppliers, which those suppliers reasonably treat as highly confidential business information and trade secrets.

supply chains.[57] In addition, many trusted suppliers leverage third parties that specialize in a particular aspect of product development, design, manufacturing, engineering or marketing while selling under their own brand. Such commercial arrangements enable companies to leverage competitive advantages to foster more choice for consumers and fuel competition to provide the best possible products. These sorts of relationships must be protected from inadvertent inclusion in the "produced by" definition.

Importantly, compliance requirements should not unnecessarily overburden good faith equipment authorization participants. The current attestations that certify that equipment is not covered are sufficient.[58] Requiring a written and signed list of *any and all* entities that produced the device for which equipment authorization is sought is unnecessarily burdensome, duplicative of the present attestation rules, and opens another vector to the release of highly confidential supplier information given the current state of the FCC's Equipment Authorization System database.[59] The FCC's marketing and enforcement precedent provides assurance that applicants will be held responsible for their attestations. In any event, the Commission cannot vet every supply chain of every product in the ecosystem as a practical matter.

B. The Proposed Electrically Identical Disclosure and Separate Authorization Requirements Are Unworkable and Unnecessary

The electrically identical disclosure and separate authorization requirements proposal would impose a significant operational burden by shifting compliance from technical hardware tracking to comprehensive entity disclosure, antithetical to the common practices of modern

[57] For example, if "Company X" requires a specific component to be present in third party devices to interoperate with their own.
[58] *See* 47 CFR §§ 2.911(d)(5)(ii), (d)(6); 2.929(c)(2); 2.938(b)(2).
[59] *Third FNPRM* ¶ 135 (proposing a signed list of producing entities); *see also id.* ¶ 172 (brand and model disclosures).

technology supply chains.[60] Even for the same model of device, the full scope of software and design entities or the multi-tier subcontractors can vary depending on the time of year, the customer involved, or the circumstances of individual contractors and subcontractors. Units of the same U.S. model may have components from different vendors from various parts of the world. This is necessary for trusted suppliers to reflect changing market conditions and compete successfully with peer companies, including those from adversary states.

Identifying and providing new certifications for all "electrically identical" products across brand portfolios would require a massive data consolidation effort across siloed business units. Requiring a company to obtain signed legal attestations from a global supply chain would significantly increase administrative costs, delay time-to-market and risk the exposure of confidential strategic partnerships. Typically, companies submit details about a product series, rather than a particular model, and market it under multiple model names if the models have the same hardware functionality. If the devices have different functionality, however, they get a separate grant. If the Commission requires separate authorizations for every rebranded model, trusted suppliers will face massive increases in filing fees and laboratory testing costs. Instead of one FCC ID for a global platform, companies would regularly be required to manage three or four separate certifications for the same physical hardware, depending on the branding.[61]

[60] *Id.* ¶¶ 136-38 (seeking comment on disclosure of all electrically identical products, brands, models, and related grantees, and on requiring separate authorizations).

[61] A single-ID "family of products" reflects how devices are designed/marketed today. *See* Letter from Paul Margie, Harris, Wiltshire & Grannis, LLP, Couns. to Apple Inc., to Marlene H. Dortch, Sec'y, FCC, ET Docket No. 15-170, at 2 (June 12, 2017) ("Apple Letter") (noting that a "family of products" under a single FCC ID "reflect[s] how many of today's RF devices are designed and marketed" and improves efficiency").

Such a departure from the current equipment authorization rules would undermine trusted manufacturers' ability to compete globally even as the Trump Administration seeks to promote U.S. companies abroad and counter national champions from adversary countries.[62]

C. The Commission Should Not Extend Covered List Prohibitions to Software and Other Components Absent a Specific Determination by an Enumerated Source

The Secure Networks Act does not empower the Commission to extend prohibitions to *all* components of a producer/provider on the Covered List absent a specific determination by an Enumerated Source, even if such a ban were "simpler and easier to comply with."[63] Many components (*e.g.*, non-logic-enabled hardware components) do not pose an unacceptable risk no matter where or what entity they are produced by. Congress explicitly directed the FCC to:

> place on the [Covered] list … any *communications* equipment or service, *if and only if such* equipment or service (1) is produced or provided by any entity, if, based exclusively on the determinations [of Enumerated Sources] … such equipment or service produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and (2) is capable of (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications services to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.[64]

This statutory text shows the emphasis Congress placed on targeting equipment and services that (i) pose a truly "unacceptable" risk and (ii) provide an actual vector for exploitation by foreign

---

[62] *See, e.g.,* Remarks of Olivia Trusty, Comm'r, FCC, "Building Global Spectrum Trust: Cooperation, Openness, and the Path to WRC-27," at the 14th Americas Spectrum Management Conference (Oct. 30, 2025); Letter from Alliance for Automotive Innovation, Consumer Technology Association, et al., to Brendan Carr, Chairman, FCC, and Jeffrey Kessler, Under Sec'y of Com. for Indus. & Sec., WC Docket No. 18-89, OET Docket No. 21-232, OEA Docket No. 21-233 at 1-2 (Sept. 4, 2025) (misaligned rules would "stifle American innovation and leadership, challenge U.S. competitiveness and relevance in the global market").

[63] *Third FNPRM* ¶ 148 (asking whether to extend prohibitions to all components of a Covered List producer/provider).

[64] Secure Networks Act § 2(b), 47 U.S.C. § 1601(b) (emphasis added).

adversaries. It also underscores that the Commission must look to Enumerated Sources to make such a risk determination. The FCC does not have the authority to *independently* determine whether, for example, "devices that have a supply chain dependency on Covered List entities for components pose national security risks."[65]

Given the very explicit, recent direction from Congress to add to the Covered List only named "communications equipment or service" produced by the specific entities to the Covered List, the Commission may not rely on the Secure Networks Act, Secure Equipment Act, or older generalized grants of authority to adopt additional, sweeping component bans.

For the same reasons, the Commission should not independently expand existing Covered List prohibitions to software and/or firmware produced or provided by a Covered List entity.[66] As noted in the *Third Order*, the Commission has so far declined to adopt such a rule, given the lack of support in the record and challenges with enforcement and oversight.[67] Determining whether a software or firmware component was "produced or provided" by a Covered List entity can be difficult if not infeasible, particularly where software incorporates multiple third-party components or is modified by another manufacturer. Modern software also often incorporates open-source libraries, third-party APIs, and code developed by global contractors. Tracking whether any of these contributors are "entities on the Covered List" or are "controlled by" such entities is likely impossible with respect to open-source software built up over decades.[68] Unlike

[65] *Third FNPRM* ¶ 148.
[66] *Id.* ¶ 150 (asking whether to extend prohibitions to a Covered List entity's software and firmware).
[67] *Third Order* ¶ 30 (declining to adopt a software/firmware prohibition given the lack of record support).
[68] *See* Bur. of Indus. & Sec., *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 90 Fed. Reg. 5360, 5376-77 (Jan. 16, 2025) (declining to limit an exclusion for open-source software because not even "BIS is not well placed to arbitrate the validity of individual open-source contributors and rather relies on the inherent structure and transparency of open-source software to identify potential security compromises by malicious actors").

hardware components, software "production" is fluid and continuous (updates, patches, etc.), making a one-time certification difficult to maintain.

If the FCC determines that software or firmware restrictions are necessary, at minimum, any rule should be narrowly limited to software or firmware specifically identified as presenting a national security risk or that is directly controlled or distributed by a Covered List entity.

V. SEVERAL PROPOSALS IN THE *THIRD FNPRM* WOULD UNDERMINE THE TECHNOLOGY INNOVATION PROCESS WITHOUT COMMENSURATE BENEFIT

Any new requirement must be justified by a demonstrated, commensurate security benefit and narrowly tailored to it. CTA supports the Commission's objective of enhancing security and ensuring compliance via its equipment authorization rules; however, several proposed measures in the *Third FNPRM* would impose substantial burdens without delivering meaningful benefits to aid the Commission's implementation of Covered List prohibitions.

A. A Measured Approach Is Warranted as the FCC Moves Forward

CTA encourages the FCC to take a measured approach to changing the Part 2 equipment rules. Any FCC action should advance national security objectives while protecting proprietary information, minimizing unnecessary administrative burdens, and preserving the competitiveness of U.S. manufacturers in the global marketplace. The Administration astutely recognized in the National Security Science and Technology (S&T) Strategy that "to remain the world's most scientifically and technologically advanced and innovative country" and "legal, policy, and structural factors must be addressed to maximize the options space for U.S. strategy."[69] The Strategy emphasizes that (i) "[e]fforts to protect sensitive S&T must protect Americans' rights and liberties *without unduly slowing the pace of innovation*;" (ii) "[e]xcessive regulation and

[69] National Security Science & Technology Strategy, The White House, at 2-3 (Aug. 2026), https://www.whitehouse.gov/wp-content/uploads/2026/08/NSSTS-082026.pdf.

inefficient legacy policies must be changed or eliminated so that they do not inhibit the ability of American industry to contribute to national security needs;" and (iii) "[t]he Federal Government must partner effectively with the private sector, recognizing that the private sector contributes critical capabilities that the government does not possess."[70]

To that end, any final rules adopted in this proceeding should be grounded in a demonstrated security benefit, supported by a clear risk-based framework and accompanied by robust safeguards to prevent competitive harm, protect intellectual property and maintain the integrity of the communications equipment ecosystem. Indeed, any requirements should be narrowly tailored, risk-based and limited to information that is necessary to address identified national security concerns. Overregulation risks ceding ground to foreign competitors and eroding the U.S. innovation and global technology leadership that the Commission's streamlined equipment-authorization framework has long advanced.

B. Mandating HBOMs and SBOMs Would Impose More Costs Than Benefits

As previously explained in the record, mandatory component-level disclosure, such as a hardware bill of materials (HBOM) and/or software bill of materials (SBOM), imposes burdens that dwarf any incremental security benefit and is unnecessary to enforce Covered List prohibitions.[71] Imposing these mandates would also handicap the very American innovation and

[70] *Id.* at 3 (emphasis added).
[71] *See*, *e.g.*, Comments of the Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233, at 17 (Sept. 20, 2021) (benefits of a detailed "parts list" are "likely minimal and would be swamped by the prospective burdens") (CTA 2021 Comments); Reply Comments of the Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233, at 3 (May 8, 2023) (attestation requirements "would introduce myriad inefficiencies and increase costs without necessarily addressing any underlying risk").

global technology leadership the Commission seeks to protect, and may even provide bad actors with new vectors of attack.[72]

1. MANDATING HBOM AND SBOM DISCLOSURES WOULD PRESENT MAJOR CHALLENGES AND MAY UNDERMINE THE COMMISSION'S GOALS

Requiring the submission of HBOMs and SBOMs raises significant concerns regarding the protection of proprietary information, intellectual property, cybersecurity and supply chain security, especially when the Equipment Authorization System is not updated in parallel. The submission of HBOMs and SBOMs would create far more risks of harm to innovators than potential benefits from hypothetical risk mitigation. Most importantly, mandating HBOMs and SBOMs may undermine national security goals.

HBOMs and SBOMs frequently contain highly sensitive technical and commercial information that reflects years of engineering effort, substantial research and development investment, and significant competitive differentiation. Depending on the level of detail required, these materials may reveal: product architectures and design methodologies, component selection strategies, supplier and sourcing relationships, software frameworks, libraries and dependencies, security implementation approaches and system configurations, manufacturing and integration practices and proprietary technology development investments. This information often constitutes trade secrets and confidential commercial information that provide manufacturers with a competitive advantage in global markets. Disclosure of such information,

[72] The *Third FNPRM* proposes to require applicants to submit a written and signed HBOM and SBOM at the time of certification, to disclose the producer and place of production of the device and each component, and to update those submissions within 30 days of any change. *Third FNPRM* ¶¶ 139-46.

even within a government reporting framework, increases the risk of unauthorized exposure, misuse or inadvertent release.[73]

A mandatory HBOM would conflict with how manufacturers manage their hardware supply chain, both before a product is authorized and during production. Manufacturers routinely qualify alternate sources and substitute components in response to capacity constraints, allocation, end-of-life, quality and cost. Requiring them to identify every component supplier, underlying producer, and manufacturing location would demand sustained coordination across engineering, operations and regulatory teams, as well as factories and third-party manufacturers. Worse, making an otherwise-qualified substitution trigger a new filing simply because the source or country changed would increase single-source exposure and reduce supply-chain resilience—the opposite of the Commission's goal. The proposed 30-day update requirement compounds the problem, because resilience depends on the ability to shift quickly among alternatives that have been qualified and validated in advance. The equipment authorization process already provides the Commission with detailed technical information about every device, including circuit descriptions, block diagrams, schematics and internal photographs. The Commission's requirements that production units be identical to the tested unit are sufficient to ensure against risks and do not require a bill of materials going forward.[74]

The SBOM proposal is no more workable. Connected devices receive operating system, firmware, driver, third-party library, open-source and security updates throughout their lives, so validating and certifying an authoritative regulatory SBOM would be a continuous, not a one-

[73] A detailed HBOM containing component manufacturers and production locations would provide substantial insight into a company's product architecture, sourcing strategy and cost structure. Much of this information is highly confidential and competitively sensitive. Requiring disclosure when this information is not needed to achieve the Commission's goals is not in the public interest.
[74] 47 C.F.R. §§ 2.906(b); 2.907(b).

time, undertaking. Where an operating system is licensed to third-party manufacturers, dozens of parties may contribute to the BOM chain, and no manufacturer can account for the open-source contributions it neither controls nor tracks.

Even if device grantees could overcome the practical challenges of complying with the HBOM and SBOM proposals, the costs will be significant and flow to consumers. The relevant cost is not simply the labor required to produce an HBOM or SBOM file, but also supplier and sub-tier data collection, engineering validation, regulatory/legal review, internal certification and recurring updates throughout the product lifecycle.

The proposed requirement could also create unintended competitive disadvantages for compliant manufacturers. Submission of detailed HBOM and SBOM disclosures can provide a roadmap to product designs, technology selections and supply chain strategies that have been developed through substantial investment and innovation. Competitors, both domestic and foreign, may be able to infer significant aspects of a manufacturer's product development strategy from detailed material disclosures. This risk is particularly acute in highly competitive sectors where differentiation is often driven by proprietary component selection, software architecture and integration methodologies rather than the underlying functionality of the finished product. As a result, broad reporting requirements may have the unintended effect of weakening incentives for innovation and reducing the value of intellectual property developed by grantees that invest heavily in product security, reliability and performance.

Comprehensive hardware and software inventories could provide valuable intelligence to counterfeiters seeking to replicate authentic products. Access to detailed component and software information may enable bad actors to manufacture counterfeit devices that more closely resemble legitimate products, making detection and enforcement efforts substantially more difficult. Such

outcomes could undermine: (i) consumer confidence and trust, (ii) product quality and reliability, (iii) intellectual property protections, (iv) brand integrity, (v) product authenticity verification efforts and (vi) broader supply chain risk management objectives. The purported supply chain transparency of requiring HBOMs and SBOMs may inadvertently facilitate more sophisticated counterfeiting activities, increase risks throughout the communications equipment ecosystem and raise enforcement costs for government.

2. HBOMs and SBOMs are Unnecessary to Effective Enforcement of Covered List Prohibitions

The Commission's existing enforcement mechanisms are sufficient to ensure equipment authorization applicants and holders remain accountable for any Covered List equipment in their products. Written and signed attestations place the burden of supply chain verification onto the party applying for the equipment authorization and establish liability for any false representations regarding Covered List equipment in the product. It would be economically and logistically infeasible for the Commission itself to investigate the origins and components of every single RF device submitted for authorization. Indeed, the Commission's existing rules recognize this and already rely on attestations to police Covered List compliance.[75] CTA and others have long explained that attestations—not component-level disclosure—are the appropriate and sufficient tool.[76]

3. If the Commission Nevertheless Decides to Mandate HBOMs and SBOMs, It Should take Steps to Mitigate Resulting Harms

If the Commission nevertheless imposes requirements to file HBOM and SBOM documentation, the agency should:

[75] *See* 47 C.F.R. §§ 2.911(d)(5)(ii), 2.911(d)(6); 2.929(c)(2); 2.938(b)(2).
[76] *See, e.g.*, CTA 2021 Comments at 16-17.

- Adopt a similar approach to other FCC cyber and supply chain rules that require the entity to maintain a plan (in this case HBOM/SBOM) but only supply it to the government when necessary and upon request.

- Adopt a simple HBOM model/template that directly reflects the FCC's component-level restrictions—*i.e.*, limit disclosure to producer/provider-based Covered List categories and require a record of which entities produced each "logic bearing hardware component" and each logic bearing hardware component's country of origin.

- Avoid requiring proprietary supply chain information that does not directly relate to the FCC's national security objectives—*i.e.*, do not require comprehensive disclosure of all hardware and software elements.

- Permit manufacturers to provide information based on reasonable supply chain due diligence. Existing supply chain risk management, secure development and vulnerability management frameworks should be leveraged wherever possible to avoid duplicative reporting obligations.

- Establish a materiality threshold for changes that require reporting, rather than requiring reporting within 30 days of *any* change, and do not require compliance with any reporting requirement prior to updating the FCC's website and databases to appropriately protect this highly sensitive information.[77]

- In cases where the operating system is licensed to third parties, clearly define the boundaries of each party's responsibilities.

The FCC should also exempt finished components, including integrated semiconductors, from any granular sub-component HBOM disclosure. Semiconductors are highly integrated products that incorporate intellectual property, design elements and sub-components from numerous suppliers across extensive global supply chains. Requiring downstream companies to identify and disclose the precise design and manufacturing locations of every sub-component within an integrated circuit would impose significant compliance burdens while providing limited incremental security value. The Commission should instead permit manufacturers to provide a high-level attestation that integrated components comply with the Commission's

[77] Regardless whether the FCC opts to mandate filing of HBOM or SBOM documentation, which it should not, the agency should improve the Equipment Authorization System as described elsewhere in these comments and ensure automatic confidential treatment of sensitive certification exhibits.

requirements and do not originate from entities included on the Covered List. This approach is consistent with CTA's prior comments explaining that tracing the lineage of every component is often difficult or impossible and that applicants should be permitted to rely on suppliers' certifications, and with the longstanding distinction—recognized by the Commission and urged by other commenters—between finished equipment and the components integrated into it.[78]

In addition, all HBOM and SBOM submissions should be automatically treated as confidential business information and protected from public disclosure, absent an extraordinary showing of need. For years, commenters have requested the Commission update its web portal and policies to provide automatic confidential treatment to sensitive certification exhibits, and the Commission's rules already withhold such exhibits from routine public inspection.[79]

The Commission should also explicitly prohibit publication of any HBOMs and SBOMs through public databases, routine disclosures, production requests or other mechanisms that could expose proprietary information. The FCC has historically recognized the importance of protecting confidential business information under its rules and in the equipment authorization process, including Sections 0.457 and 0.459,[80] and long-term/permanent confidentiality for

[78] *See* 47 C.F.R. § 15.101(d)(1); Comments of the Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233, at 12, 14 (Apr. 9, 2023) (tracing the lineage of a particular component "could range from difficult to impossible," and applicants should be "permitted to rely upon certifications from suppliers"); Reply Comments of the Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233, at 10 (Oct. 18, 2021) (policymakers "should defer to existing self-attestation and conformity assessments by suppliers and vendors"); Comments of Panasonic i-PRO Sensing Solutions Corp., ET Docket No. 21-232, EA Docket No. 21-233, at 8 (Sept. 20, 2021) (requesting that the FCC preserve the distinction between "equipment" and integrated "components"); Comments of Sony Group Corp., ET Docket No. 21-232, at 1 (Dec. 29, 2025) (suggesting the Commission "not expand the regulations to broadly encompass component parts installed in finished products") (Sony Comments).
[79] *See* Comments of Google Inc., ET Docket No. 15-170, at 14-17 (Oct. 9, 2015) (urging automatic and expanded confidential treatment of certification-application exhibits, including schematics, block diagrams, operational descriptions, and parts lists) (Google Comments); Comments of Samsung Electronics America, Inc., ET Docket No. 15-170, at 7-8 (Oct. 9, 2015) (supporting automatic confidential treatment of such exhibits); *see also* 47 C.F.R. § 0.457(d).
[80] 47 C.F.R. §§ 0.457, 0.459.

certain application materials. Similar protections are reflected in FOIA Exemption 4[81] and the Trade Secrets Act.[82] Any reporting framework should be designed consistent with these longstanding principles to ensure that commercially sensitive information remains adequately protected. Finally, the Commission should limit access to HBOM and/or SBOM submissions to authorized FCC personnel and approved reviewers with a demonstrated need to know.

C. Self-Approval Procedures Appropriately Simplify the Equipment Authorization Process Allowing the Commission and the Consumer Technology Industry to Focus Resources

The Commission must protect the SDoC process and should not require every device in a Covered List sector to undergo full certification. Nor should it require all devices authorized through the SDoC process to be registered with the FCC and assigned a unique identification number that would be publicly available. As explained in previous comments, the SDoC option for equipment authorization is a valuable, useful and secure method for manufacturers of unintentional radiators (and certain intentional radiators) to quickly bring equipment to market and avoid burdens and costs of the certification regime.[83]

In contrast to the burdens the *Third FNPRM*'s proposals would impose, the benefits of further restricting SDoC procedures are uncertain. At a minimum, the proposal to force more devices subject to SDoC into certification would increase the cost and complexity of equipment approval for such devices. Moving products from SDoC to a third-party approval process would introduce harmful schedule variability into product launches—in addition to the increased costs

[81] 5 U.S.C. § 552(b)(4).
[82] 18 U.S.C. § 1905.
[83] *See, e.g.*, CTA 2021 Comments at 19 (noting that the SDoC option "is a valuable and useful method for manufacturers of unintentional radiators (and certain intentional radiators) to quickly bring the equipment to market and avoid burdens of the certification regime"); Comments of Consumer Technology Association, ET Docket No. 24-136, at 2 (Sept. 3, 2024) ("The SDoC process for equipment authorization has robust protections in place. Importantly, *entities* identified on the Covered List are prohibited from using SDoC.") (CTA 2024 Comments) (emphasis added).

of paying an accredited lab to test the product and then a Telecommunications Certification Body (TCB) to review those tests at a time of constricting lab availability. Even short approval delays can cascade into factory holds, missed vessel bookings, higher costs due to expedited freight needs, retailer timing issues, and lost sales.[84] Together, the consequences would be delays in and higher prices for new innovations reaching American consumers.

The FCC should retain the existing SDoC framework and should not impose universal registration or new labeling requirements, which would impose significant collection, reporting, and disclosure costs under the Paperwork Reduction Act, easily exceeding millions of dollars and many thousands of man-hours.[85] These burdens would apply to large and small entities alike. Further, in addition to the long-needed Equipment Authorization System updates already required to support the Commission's current rules, let alone proposals, adopting the SDoC proposals would likely require another portal that can support the extraordinarily high volume of new filings this would mandate. If the registration requirement is ultimately adopted, it should be limited to narrowly defined categories presenting a demonstrated national security concern and should function as a simple notification mechanism rather than a substantive approval process.

D. Encumbering the Lawful Marketing of Authorized Devices Will Drive Up Compliance and Consumer Costs Without Mitigating Security Risks

The *Third FNPRM* proposes to impose new regulatory requirements that will likely chill the marketing of authorized devices and make doing so more costly.[86] Manufacturers and responsible parties comply with extensive labeling, user documentation and, in some instances,

[84] *See e.g.*, CTA 2024 Comments at 2; CTA 2021 Comments; Google Comments at 2 (noting that a single self-approval process "would allow faster authorization of products at lower expense").
[85] *See* Paperwork Reduction Act of 1995, 44 U.S.C. §§ 3501-21; *Third FNPRM* ¶ 216 (seeking comment on the costs of database changes and reporting).
[86] *Third FNPRM* ¶¶ 176-81 (proposing new consumer-facing marketing and labeling requirements).

online posting requirements under the existing FCC rules.[87] 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 or FCC logo would impose unreasonable burdens with likely little additional benefit. Many authorized devices do not require FCC IDs or an FCC logo, such as those that are authorized via an SDoC.

CTA has repeatedly highlighted the consumer benefits of simplified and digitalized labeling and urges the Commission to continue to move towards—not away from—more effective disclosures.[88] Further labeling or point-of-sale disclosure requirements will be difficult to implement consistently across retail channels, and the *Third FNPRM* cites no data to show that additional requirements will enhance compliance or enable better consumer understanding. Raising the potential for consumer confusion that the FCC lifted a labeling requirement for the FCC logo less than a decade ago. Specifically, in 2017, the FCC logo went from being required for certain products authorized by the now defunct Declaration of Conformity process to being voluntary for SDoC-authorized devices. Another change to the FCC rules would muddy understanding, leading to a market that could contain older certified products with an FCC ID and no FCC logo, newer certified products with an FCC ID and FCC logo, SDoC products that legitimately have or do not bear an FCC logo, and even some older legacy DOC authorized products with an FCC logo—all of which would be legally displaying the symbol. New labelling requirements would also cause unnecessary confusion as the FCC launches the U.S. Cyber Trust Mark.[89] In short, changing the meaning of the FCC logo again may actually undercut consumers'

[87] *See, e.g.*, 47 C.F.R. §§ 2.925, 2.1077, 15.19, 15.21, 15.27, 15.105, 15.257, 20.19(f)-(h).
[88] *See* Labeling Policy, CTA, https://www.cta.tech/advocacy/labeling-policy (last visited Sept. 4, 2026).
[89] *See* Comments of the Consumer Technology Association, ET Docket No. 21-232, at 10-11 (Jan. 5, 2026) (noting CTA "has repeatedly highlighted the consumer benefits of simplified and digitalized labeling") (CTA 2026 Comments); Letter from Rachel Nemeth *et al.*, Vice President, Regul. & Gov't

understanding of a device's security posture and complicate the efforts of retailers and manufacturers to explain the significance of the markings on their devices, on boxes and in product listings.[90]

As the Commission recognizes, online materials have finite "valuable [display] real estate."[91] To avoid regulatory ambiguity, the Commission should confirm that the online point of sale refers to the "product listing page" where complete product specifications are listed and consumers are provided with a call to action (*e.g.*, "Add to Cart" or "Buy Now") rather than other materials such as transactional checkout flows (*e.g.*, shopping cart drawers or order review screens) where disclosures can create confusion and transactional friction. Clarification here will assist online marketplaces in complying with the Commission's rules.

The Commission should refrain from merging FCC ID display obligations for its two distinct categories of online marketplaces established in the *Third Order*:[92] (1) online marketplaces that sell devices themselves or have access/title to the products versus (2) online marketplaces that sell devices on behalf of third-party sellers without access/title to the products. Any requirement imposed on the latter category should be limited to ensuring that the third-party seller-provided FCC ID is valid and requiring that the third-party seller certify the accuracy of the information supplied.[93] The third-party seller should *not* have to verify the accuracy of the

---

Affs., Consumer Technology Association, to Marlene H. Dortch, Sec'y, FCC, WC Docket No. 18-89, ET Docket No. 21-232, at 2 (June 4, 2026) (showing CTA "championing the U.S. Cyber Trust Mark").

[90] *2017 Equipment Authorization Order* ¶¶ 17-19 (eliminating the mandatory FCC logo requirement and permitting voluntary use of the logo as a visual indicator of compliance for devices authorized under the SDoC); *see* 47 C.F.R. §§ 15.19, 18.209. The compliance date for additional labeling and disclosure requirements related to the hearing aid compatibility of wireless handsets is later this year, already increasing the FCC-required information consumers must wade through to use their consumer technology. 47 C.F.R. § 20.19(f).

[91] *Third FNPRM* ¶ 215 (recognizing that online materials have finite display "real estate").

[92] *Third Order* ¶ 74 (establishing two categories of online-marketplace FCC ID display obligations).

[93] *Id*.

FCC ID,[94] which would unduly burden this category of online marketplace that does not have possession of the equipment for sale. It would also present a significant barrier to entry for consumers and small business sellers.

Imposing new SDoC verification regulations on retailers and online marketplaces would significantly increase regulatory compliance burdens and put such entities in the impossible position of determining whether a device should even be authorized via SDoC.[95] The scope of affected devices is huge, there is no third-party database for SDoC to search and several reasons why a digital device may not be authorized via SDoC.[96] Additionally, a requirement for retailers and online marketplaces to obtain proof of licensure and verify that information prior to completing a sale of certain devices such as amateur radio equipment[97] would be technically infeasible to implement. ULS database latency, database downtime or even minor discrepancies in buyer name or address matching could disrupt checkout flows and prevent lawful transactions.

Failing to preserve the newly-created exemptions for small sellers and used/resale devices would backtrack on the Commission's exemptions to its rule.[98] Imposing the Commission's FCC ID display rules on a seller with "an aggregate total of $5,000 or more in gross revenues" would be a barrier for small sellers to list products on the popular internet marketplaces.[99]

---

[94] *Third FNPRM* ¶ 168 (proposing to require marketplaces to verify FCC ID accuracy).
[95] *Id.* ¶ 168 (proposing SDoC verification obligations on retailers and online marketplaces).
[96] *See, e.g.*, 47 C.F.R. 15.101(a) (allowing several types of unintentional radiators to be equipment authorized using the SDoC or certification procedure). As noted above, the lack of a central database appropriately reflected the diversity of SDoC devices, their low interference potential, and the robust measures already in place to ensure device integrity.
[97] *Third FNPRM* ¶¶ 174-75 (proposing proof-of-licensure verification for certain licensed devices, such as amateur radio equipment).
[98] *Id.* ¶ 168 (addressing exemptions for small sellers and used/resale devices).
[99] *See* ¶ 236 (seeking comment on the potential effects of the *Third FNPRM*'s proposals on small businesses).

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 lack access to regulatory authorization or compliance records held by manufacturers. Requiring importers, distributors and other sellers to repeatedly re-verify the authorization status of inventory would create substantial logistical and administrative burdens. 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. Indeed, frequent checks would be unfeasible for high-volume distributors. Re-verification would delay product movement through the supply chain, affecting availability and market timing. 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.

E. Requiring Renewals of Equipment Authorization Diverts Resources from New Devices to Old Ones Without Materially Enhancing Compliance

As discussed in previous phases of this proceeding, 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 equipment authorization.[100] The consumer technology industry relies heavily on the FCC's established "test-once, sell-forever" policy to continue innovating new devices rather than constantly looking backward. Many long-lifecycle products remain unchanged for years, providing important value for consumers that have, to date, not worried about a government-imposed expiration date. 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.

[100] CTA 2026 Comments at (industry "relies heavily on the FCC's established test-once, sell-forever policy," and expiration dates "would be a sea-change in the Commission's longstanding approach to equipment authorization").

Recertifying devices solely due to an arbitrary time limit would divert engineering resources without improving safety or compliance while likely generating confusion. 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.[101]

Many certified and SDoC devices remain in service well beyond ten years, often because replacement is costly, disruptive or subject to its own separate regulatory approval processes. Even a ten-year term is particularly disruptive for long-lifecycle industrial, medical and infrastructure equipment. And, some segments, like aviation or industrial controls, have equipment that is manufactured and fielded for decades and already subject to ongoing support requirements.[102] As such, the Commission should avoid fixed term limits, with authorizations remaining valid unless the FCC identifies a specific compliance, interference, safety or national security basis for limiting or revoking it.[103] If any fixed term limit is imposed, it should be limited to authorization for future manufacturing/marketing and should not interfere with continued operation or the ability to provide software and security updates to devices already in

[101] *See, e.g.*, *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, Second Report and Order, Order on Reconsideration, and Second Further Notice of Proposed Rulemaking, ET Docket No. 24-136, FCC 26-28, ¶ 76 (rel. May 1, 2026).
[102] *See* CTA 2026 Comments at 11-12 (opposing expiration dates and time limits and explaining that many long-lifecycle products remain in service well beyond ten years).
[103] *See, e.g.*, Sony Comments at 3 (recommending the FCC "refrain from introducing expiration dates," which would force needless renewals for "long-lifecycle products … even when no changes affect authorization status").

use. In addition, any new rules requiring re-authorization or a streamlined renewal raise several important questions both about implementation and the significant costs to consumers, manufacturers and others in the marketplace: How will older devices be assessed and by whom? What applicable technical and other rules should apply—the rules in effect at the time or the original rules against which the devices were certified? May consumers continue to use their devices? Can inventory in retail locations and warehouses be sold? Can used devices be sold?

VI. IMPLEMENTING THE PROPOSED REGULATIONS AND RESTRICTIONS WILL COST SIGNIFICANT PRIVATE AND PUBLIC RESOURCES

As discussed throughout this comment, the industry anticipates that both consumers and businesses will incur significant costs associated with the proposals.[104] Further, the Commission will also require significant time and resources to implement the proposals in the *Third FNPRM*. As just one example, eliminating pre-authorization research, development, trialing, demonstrating and other importation and marketing will greatly increase the costs of bringing *any* device to the market in the United States while reducing the availability of devices. Meanwhile, several of the reporting proposals would require significantly new government expenditures.[105] In many cases, these proposals bear little to no relation to the Commission's national security objectives. In some cases, the proposals may actually increase national security risks. Implementation of these requirements cuts against the efficiencies achieved in the Commission's *Delete* proceedings.

Direct compliance costs on industry are almost certain to be in the billions, and these costs will either be passed along to consumers or dissuade innovators from offering their devices to U.S. consumers. The Commission estimated its *one* new set of FCC ID display rules to cost

[104] *Third FNPRM* ¶ 233 (seeking comments on the costs of the proposed rules).
[105] *See id.* ¶¶ 216, 233 (seeking comment on costs, including the costs of modernizing the Equipment Authorization System).

nearly $300 million in one-time implementation costs and $40 million in recurring annual costs.[106] The *Third FNPRM* seeks comment on eliminating the small business exemptions to those new rules and imposing numerous other display, disclosure, reporting and warning requirements.

CTA has previously supported the modernization of the Equipment Authorization System database and requests that the Commission proceed to update the database, while recognizing this is likely to be a costly undertaking.[107] Among other things, any requirements to file additional and detailed highly-confidential materials such as HBOMs and SBOMs would require an updated and hardened FCC database and portal against cyberattacks and breaches.[108] Likewise, increasing the volume and sensitivity of information shared with TCBs would also increase their cybersecurity needs as well as generally increase the attack surface for foreign adversaries and other bad actors looking to steal intellectual property and trade secrets and create counterfeit devices. This would, in turn, further increase certification costs.

Beyond cost, database modernization helps to address basic workability challenges in today's rules: a company may lawfully market or import a device only if its authorization has not been limited, yet the database does not currently show whether a given grant has been limited, revoked or withdrawn—leaving good-faith sellers to satisfy a condition they cannot readily verify. Any new registration related to devices approved via SDoC would likely require the Commission to establish a new web portal.

---

[106] *Third Order* ¶¶ 110-11.
[107] *See* Letter from J. David Grossman et al., Vice President, Pol'y & Regul. Affs., Consumer Technology Association, to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232 (July 13, 2026) (supporting modernization of the Equipment Authorization System database to enable the verification that the Commission envisions); *Third FNPRM* ¶ 216.
[108] *See* 47 C.F.R. § 0.457(d); *see also* Comments of the Consumer Technology Association, ET Docket No. 24-136 (Sept. 3, 2024) (addressing confidential treatment of equipment authorization application materials).

VII. APPROPRIATE TRANSITION PERIODS GROUNDED IN MARKET REALITIES ARE CRITICAL TO ENABLE COMPLIANCE AND PROMOTE CONTINUED U.S. TECHNOLOGY LEADERSHIP

Transition periods mitigate risks by enabling important maintenance and updates, along with other national and economic security benefits. There should be a sufficient transition period, such as three years, for any new requirement that is ultimately adopted.[109]

Over the last year, the FCC's Covered List prohibitions have been shifting on an almost monthly basis, expanding beyond finished products by specifically named entities to products with components from such entities, and more broadly, classes of products manufactured in foreign countries (including by trusted manufacturers based in the U.S. or allied countries). Some of these designations are contingent on the particular use case of a product (*e.g.,* video surveillance equipment that is used for public safety, national security or critical infrastructure), and entries change by new national security determinations (e.g., power inverters, toy drones) or via Conditional Approvals (*e.g.*, drones and consumer routers, which may be exempted from the Covered List by DOW or DHS for a period of time).[110] The FCC has also granted limited waivers in certain instances while further restricting the importation and marketing of covered equipment in others.[111] The Administration may send the FCC additional national security

[109] *Third FNPRM* ¶ 234 (seeking comment on appropriate transition periods). New rules bifurcating the Covered List and allowing additional permissive changes to covered list should be effective when any new Order is effective, such as thirty days after publication of the new Order in the Federal Register.
[110] For example, the Administration recently added certain power inverters to the Covered List and issued a second National Security Determination modifying the scope of covered power inverters less than one month later. *See First Power Inverters PN*; *Second Power Inverters PN*.
[111] *See, e.g.*, *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered Routers*, Public Notice, ET Docket No. 21-232, DA 26-286 (OET rel. Mar. 23, 2026); *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered UAS and UAS Critical Components*, Public Notice, 41 FCC Rcd 305 (2026); *AT&T Services, Inc.*, Order, ET Docket No. 21-232, DA 26-491 (rel. May 15, 2026); *NCTA – The Internet and Television Association*, Order, ET Docket No. 21-232, DA 26-571 (rel. June 9, 2026); *Verizon Communications Inc.*, Order, ET Docket No. 21-232, DA 26-641 (rel. June 26, 2026); *Public Safety and Homeland Security Bureau and Office of Engineering and Technology Prohibit the*

determinations on components that will change the status of any number of products sold on e-commerce sites.

Adjusting to any new restrictions will require significant resources in both time and money in both direct costs for new software development, tracking systems and reassigning employee responsibilities as well as indirect costs as additional employee training and legal support. Absent reasonable transition timelines, new restrictions could shock supply chains, prevent secure devices from coming to market or continuing in the market and exacerbate resulting price increases that must account for increased compliance costs. 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 parts years in advance of a product rollout. Trusted manufacturers need reasonable transition timelines to implement new 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. A key aspect of a reasonable transition period is time for continued maintenance for implicated equipment and services already in the market.[112]

Any new requirements should apply to newly authorized equipment and include a compliance period of at least three years. Previously authorized, manufactured, imported or distributed devices should be grandfathered, including after a permissible change. This is especially important with the recent trend towards production location-based bans on equipment that go into effect immediately and without notice.

Importation and Marketing of Previously Authorized Covered Communications Equipment Added to the Covered List in 2024 or Earlier, Public Notice, PS Docket No. 26-72 (rel. June 26, 2026).

[112] *See, e.g.*, Letter from Nicolas Fetchko et al., Head of Int'l Gov't Affs. & Trade Pol'y, Verizon Communications Inc., to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232, EA Docket No. 21-233, at 2 (June 29, 2023) (urging the FCC to review supply-chain impact and consult industry on transition periods "sufficient to allow the global market to adjust to avoid supply chain shortages").

CTA appreciates the Commission's work with industry to ensure that new prohibitions and rules are not applied retroactively to previously authorized products. CTA urges the Commission to continue to refrain from requiring manufacturers to retroactively reconstruct supply chain information or obtain new registrations solely because a new requirement becomes effective after a product has already been lawfully authorized and placed on the market.

Along with compliance, CTA members want to work with the Commission to optimize enforcement of the existing rules. Should the Commission adopt additional conditions for streamlined revocation, grantees should have sufficient opportunities to contest allegations of willful misstatements/misrepresentations. Revocation should remain a last resort given the likelihood that devices will be in the hands of consumers who likely will not know that they may no longer operate their devices.[113]

Relatedly, the Commission should provide advance notice of new Covered List designations—particularly the broad "foreign-produced" and production location-based designations that have taken effect immediately and without prior notice. The absence of advance notice imposes substantial and avoidable costs, forcing companies to divert engineering, compliance and legal resources away from innovation and revenue-generating activity to respond to prohibitions that become effective before affected parties can even assess their scope. A reasonable advance-notice mechanism, paired with a defined future effective date, would allow trusted manufacturers to plan supply chain and compliance adjustments—including ensuring adequate security at these new facilities to guard against IP or trade secret theft—in an orderly manner while fully preserving the government's ability to address genuine national security risks.

[113] Similarly, retailers, especially small retailers and sellers of used equipment, are unlikely to know if a device's authorization has been revoked and therefore may not be sold.

VIII. CONCLUSION

Taking a targeted, measured approach to implementing the Secure Networks Act, the Secure Equipment Act and the Commission's equipment authorization authorities is critical to effectively addressing threats from untrusted suppliers and vital to preserving the innovation environment that Americans enjoy and rely upon. The flexibility in the FCC's equipment authorization process and the regulatory streamlining this Administration has championed pave the way for more jobs and more investment in life-changing technologies across every aspect of American life. With practical transition periods, reasonable compliance standards and collaboration with industry, the Commission can improve national security without imposing unnecessary costs on consumers, retailers and manufacturers. The recommendations above will help ensure that the Commission's implementation of Covered List prohibitions promotes a unified national security posture while minimizing harms to consumers and businesses working to comply in good faith. CTA welcomes further engagement with the Commission on this important matter.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

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

/s/ Rachel Nemeth
Rachel Nemeth
Vice President, Regulatory & Government Affairs

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

September 8, 2026