1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

Via ECFS

September 28, 2026

Marlene H. Dortch, Esq.
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program—ET Docket No. 21-232*

Dear Ms. Dortch:

The Consumer Technology Association (CTA)[1] urges the Federal Communications Commission (FCC or Commission) to help consumers, the consumer technology industry, and small businesses of every kind navigate increasingly sweeping Covered List determinations by preserving pathways to bringing innovative technology to market in the United States and adjusting certain rules to the new regulatory landscape.[2]

Both the Trump Administration and numerous stakeholders agree that American technology leadership and national security are mutually reinforcing goals—both of which rely on collaboration with international partners to promote a robust base of trusted suppliers and the United States maintaining its place as the innovation capital of the world.[3] Recent national security determinations that broadly prohibit production in

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's largest 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] *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*, respectively). Unless otherwise noted, comments referenced herein were filed in ET Docket No. 21-232 on or about September 8, 2026.

[3] *See e.g.*, Consumer Technology Association (CTA) Comments at 27-28 (citing the National Security Science & Technology Strategy's direction to protect sensitive science and technology without unduly slowing the pace of innovation); CTIA Comments at 5-9 (citing remarks of Commerce Deputy Secretary Paul Dabbar on how allied scale is a critical component of the nation's 6G strategy); Association for Advancing Automation (A3) Comments at 4-7 (explaining how innovative robotics are essential to maintaining U.S. competitiveness and reestablishing preeminence in U.S. manufacturing); Commercial

any other country—including America's closest allies—undermine these goals and force businesses of every size, based in the United States as well as overseas, to weather perpetually shifting prohibitions amid an already challenging supply chain environment.[4] These actions inherently raise prices and limit availability, harming American consumers.[5]

Technology suppliers, investors, and customers across numerous sectors agree that certain proposals in the *Third FNPRM*—e.g., to bifurcate the Covered List rules, codify permissive change flexibility, and clarify key terms—will help implement these national security determinations consistently and effectively. Conversely, stakeholders emphasize that changes to existing exemptions and overbroad disclosure, certification, and reauthorization requirements would materially hinder the ability to bring innovative products to market, raise prices, and ultimately harm consumers and industry without mitigating identified national security risks.

I. The Record Overwhelmingly Agrees that the FCC's Current Approach to Early Concept and Pre-Authorized Devices Fosters Innovation

The United States is one of the best places to launch and grow a business, in part because for decades the U.S. government has worked to foster a supportive ecosystem for innovation. As anyone who has walked the floor at CES's startup hub, Eureka Park, can attest, flexibility to import and operate early concept and not-yet-authorized devices under defined circumstances provides crucial pathways for experimentation, demonstration, and evaluation.[6] This is particularly true for trade shows, which provide a controlled, concentrated environment where developers can demonstrate prototypes for potential investors, test interoperability with other devices, receive customer feedback, and identify partners. That strategic advantage is exponential for start-ups and smaller innovators, who often bridge the gap between concept and commercial success on the show floor. Today, U.S. consumers enjoy a variety of products that began as promising ideas in Eureka Park, earned recognition at CES, and became market-leading competitors through that iterative development process.[7]

For these reasons, stakeholders overwhelmingly agree the FCC should maintain and confirm existing rules that allow for limited importation, marketing, and operation of

---

Drone Alliance (CDA) Comments at 1-2 (describing the imperative for U.S. leadership in drone technology).

[4] *See, e.g.*, CTA Comments at 15-17; CTIA Comments at 9-10; Information Technology Industry Council (ITI) Comments at 2-5; Software & Information Industry Association (SIIA) Comments at 1; Telecommunications Industry Association (TIA) Comments at 6-7; CTA (@CTATech), X (July 30, 2026), https://x.com/CTATech/status/2082853441462841735?s=20.

[5] CTA is currently studying the cost of reshoring consumer technology manufacturing to the U.S. The report finds that for most consumer technology products, U.S. final assembly using imported components would increase the landed cost of those products by 5-58 percent.

[6] *See* Kinsey Fabrizio, *Protecting America's Role as the Testbed of Innovation* (Sept. 28, 2026), https://www.linkedin.com/pulse/protecting-americas-role-testbed-innovation-kinsey-fabrizio-vsave.

[7] *Id*.

unauthorized devices that empower research, development, and sales without creating national security concerns.[8] The present flexibility enables critical production milestones to occur in the United States, to the benefit of U.S. technology leadership and the Administration's onshoring goals.

II. Comments Representing Industries that Make and Sell Equipment Agree that Certain Proposals Would Increase Prices and Harm Consumers

Stakeholders across the consumer technology market and other markets that use or sell communications equipment share CTA's significant concerns that proposals to reshape the equipment authorization program more broadly will raise prices and otherwise harm consumers.[9] With so many proposals that would shift the environment from targeted new record retention requirements to a full-scale reimagining of how equipment is authorized, marketed, and remains authorized, industry cannot estimate the costs of the FCC's proposals with any degree of accuracy.[10]

Nonetheless, commenters that design, manufacture, and sell devices agree that certain proposals would raise costs far beyond any national security benefits, including but not limited to requiring: (i) full certification for all products in a Covered List sector rather than use of the SDoC process; (ii) the submission and updating of SBOMs and HBOMs; (iii) recertification of equipment after an arbitrary period of time; (iv) additional point-of-sale disclosures and labeling; (v) registration of SDoC devices; (vi) additional collection, verification, and display of FCC regulatory information in online marketplaces; and more.[11] Such steps would significantly increase compliance costs for companies, which would likely be passed down to consumers.

---

[8] *See generally* Exhibitions & Conferences Alliance, et al. Comments (letter from 100 trade associations expressly supporting a clear affirmation from the FCC that innovative pathways to import, market, and operate unauthorized devices in the United States for limited purposes remain open).

[9] *See, e.g.*, CTA Comments at 1-2; National Rural Electric Cooperative Association (NRECA) Comments at 4; Association of Home Appliance Manufacturers (AHAM) Comments at 3; Outdoor Power Equipment Institute Comments at 7.

[10] For example, the proposals discussing registration of Supplier's Declaration of Conformity (SDoC) devices range from entering some information in a database to filing full software and hardware bills of materials (SBOMs and HBOMs). *Third FNPRM* ¶ 213; *compare with id.* ¶ 143 (seeking "specific quantitative evidence on whether these estimates are reasonable, too high, or too low, and whether alternative cost estimates or methodologies should be considered"); *id.* ¶¶ 156, 175 (same). Likewise, industry cannot evaluate tradeoffs when the *Third FNPRM* does not explain how a particular proposal will benefit, e.g., national security in relation to the burdens it would impose. *See, e.g.*, *id.* ¶ 208 (asserting "[w]e believe that there may be significant value to the automatic expiration of an authorization," without indicating what that value would be or the national security threat it would mitigate).

[11] *See, e.g.,* AHAM Comments at 2-3 (expressing concern that broad disclosure requirements and duplicative HBOM/SBOM requirements would impose costs without corresponding benefits); Mobile & Wireless Forum (MWF) Comments at 6-7, 10, 24-25 (expressing concern that HBOM/SBOM requirements, SDoC registration, and equipment-authorization term limits would impose substantial and unnecessary burdens on manufacturers); ITI Comments at 7-10, 12, 23-26 (expressing concern regarding universal HBOM/SBOM filing, SDoC registration, sector-wide certification, and additional compliance burdens); USTelecom Comments at 8-12, 15-16 (expressing concern regarding the burdens associated with HBOM/SBOM reporting, sector-wide certification, and related supply-chain attestations); Wi-Fi

Particularly concerning are proposals like term limits, additional point-of-sale disclosures and other restrictions on marketing devices that could cause consumers and small businesses to inadvertently violate the Commission's rules without knowledge or intent.[12] Especially for small businesses and startups, these proposals could establish roadblocks so large that many innovations never make it into the hands of U.S. consumers.

III. The Record Agrees That New Rules to Implement National Security Determinations Should Minimize Burdens on the Equipment Authorization Process as Much as Possible

Some evolution of the equipment authorization rules is necessary to avoid costs and harms to consumers as the Commission and industry adjust to the Administration's new goals for the Covered List and its new production-based entries.[13] Any new rules should also account for the substantial progress both the FCC and industry have made towards mitigating national security threats through the Equipment Integrity proceeding, the FCC-industry Operation Clean Carts initiative, the U.S. Cyber Trust Mark partnership, and enforcement.

A. New Rules Must Provide Reasonable Transition Periods to Facilitate Compliance and Mitigate Supply Chain Shocks That Can Harm Consumers

Stakeholders have emphasized—both in response to the *Third FNPRM* and in related proceedings this year—that the global market is facing unprecedented demands for critical components as companies race to deliver emerging technologies (like AI, cloud, connected devices, and more) and as countries impose a parade of shifting restrictions.[14] New requirements could further compound these challenges.

Alliance Comments at 13-20, 34-37 (expressing concern regarding comprehensive HBOM/SBOM requirements, automatic expiration of equipment authorizations, and independent marketplace verification obligations).

[12] For example, despite Executive Order 14396 preserving its prominence, a factory worker watching "America's Game" on their TV in a few years may violate the FCC rules if the FCC adopts novel term limits and the manufacturer does not reauthorize that model. *Third FNPRM* ¶ 208 (seeking comment on a rule that would limit the operation of previously authorized devices after a certain amount of time).

[13] Although stakeholders identify fundamental problems with production location-based Covered List entries and other rules in this proceeding, CTA suggests ways to achieve the Administration's goals while imposing the minimum burdens on consumers and industry.

[14] *See, e.g.*, CTA Comments at 16-17; *see also* 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 (filed May 11, 2026); NCTA – The Internet & Television Association Petition for Expedited Waiver to Permit Targeted Class I and Class II Permissive Hardware Changes to Covered Routers, ET Docket No. 21-232 (filed Sept. 9, 2026); Verizon Communications, Inc. 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 (filed June 11, 2026); *see also* Comments of CTA, ET Docket No. 24-136, at 1-3 (June 12, 2026).

As the Commission considers next steps in response to the *Third FNPRM*, any new rules should provide sufficient time for companies to establish and implement compliance plans.[15] If the Commission adopts new disclosure requirements, particularly for SBOM/HBOM, it should ensure that systems like the equipment authorization system (EAS) database are equipped to intake and protect that information before such disclosures go into effect.[16] With respect to supply chain information, the Commission should permit applicants to provide information based on reasonable supply chain due diligence, leveraging existing frameworks where possible to avoid duplicative reporting obligations, and allow downstream providers to reasonably rely on that information as well.[17] The Commission also should take steps proposed in the *Third FNPRM* to provide necessary clarity to ensure consistent application of the Covered List prohibitions.

B. Stakeholders Broadly Agree that the Commission Should Bifurcate Its Rules Between Producer/Provider and Production Location Bans

Commenters agree that "production location-based," sectoral determinations target different risks and present distinct implementation challenges from the specific "producer/provider-based" determinations on which the existing Covered List rules are built.[18] Formalizing this distinction will enable the Commission to account for these differences, reducing disruptions to the market, businesses and consumers. Stakeholders agree the Commission should limit the application of production location-based bans to finished products identified in the underlying national security determination to avoid unclear and unworkable restrictions.[19]

C. The Record Supports Codifying Permissive Change Flexibility for Modifications in the Public Interest

Commenters further agree that the Commission should codify permissive change flexibility for software and firmware updates and for hardware modifications that do not raise national security concerns.[20] Although equating modifications to authorized

[15] *See, e.g.*, Association for Uncrewed Vehicle Systems International (AUVSI) Comments at 8; Computer & Communications Industry Association (CCIA) Comments at 29; CDA Comments at 12; CTA Comments at 44; ITI Comments at 28; National Electrical Manufacturers Association (NEMA) Comments at 4-5; TIA Comments at 20.

[16] *See, e.g.*, AHAM Comments at 4; CDA Comments at 5; CTA Comments at 43; Solar Energy Industries Association (SEIA) Comments at 19; TIA Comments at 19-20.

[17] *See, e.g.*, AHAM Comments at 4; Carnegie Endowment for International Peace Comments at 8-9; CTA Comments at 22-24; SEIA Comments at 25; TIA Comments at 14-15.

[18] *See, e.g.*, CTA Comments at 15-17; CTIA Comments at 13; NEMA Comments at 4; RoboStrategy Comments at 12-13; SEIA Comments at 18, 20-21; TIA Comments at 6-7; USTelecom Comments at 5-6.

[19] *See, e.g.*, CTA Comments at 17; SEIA Comments at 20-21. In no case should the Commission independently extend prohibitions to software and/or *all* components. *See, e.g.*, AUVSI Comments at 3; CTA Comments at 15-17; CTIA Comments at 13; NEMA Comments at 4; NTCA—The Rural Broadband Association (NTCA) Comments at 2-4; SEIA Comments at 20-21; TIA Comments at 5-7.

[20] *See, e.g.*, AUVSI Comments at 6-7; CTA Comments at 18-20; CTIA Comments at 27-28; ITI Comments at 18-19; NCTA–The Internet & Television Association (NCTA) Comments at 6-8; NEMA

devices with new authorization may have been appropriate when the Covered List was restricted to identified entities offering named equipment and services, such a broad brush is too restrictive for the sector/production location-based Covered List entries.[21] Allowing relatively minor changes without triggering new authorization requirements will avoid *de facto*, retroactive bans, support equitable, predictable application of the FCC's rules, and reduce the strains on FCC staff that are now regularly reviewing similarly situated waiver requests.[22] Although one commenter suggests the Commission "consider screening security patches while allowing for routine maintenance updates," it fails to explain how the benefits of such a step would outweigh the overwhelming administrative burden.[23] Indeed, the sheer volume of regular security updates across the broad range of products in the U.S. market would make this an infeasible task and undermine the strong public interest for both consumers and businesses in maintaining secure devices in the market.

D. The Record Cautions Against HBOM/SBOM Mandates, While Explaining the FCC Can Effectively Enforce the Covered List Bans Through Attestations and Record Retention

Technology producers across varied sectors detail challenges associated with imposing SBOM and HBOM mandates.[24] Modern technology supply chains are complex, dynamic, and global—to the benefit of resiliency and innovation. Collecting and maintaining such information is at best expensive and often infeasible, because many suppliers treat sourcing, allocation, and design information as proprietary trade secrets. Requiring disclosure of such information to the FCC would generate significant security, competition, and innovation risks; a central cache of proprietary supply chain data would be an attractive target for malicious actors, counterfeiters, and foreign adversaries. As many stakeholders note, and as expert security agencies recently corroborated, relevant standards, tools, and practices have not yet matured to support ubiquitous, automated use of HBOMs and SBOMs.[25]

However, the Commission does not need to impose SBOM/HBOM requirements to enforce the Covered List rules. As numerous stakeholders note, existing attestation and

---

Comments at 4; NTCA Comments at 8-10; RoboStrategy Comments at 14-15; SEIA Comments at 4-6; TIA Comments at 24-26; USTelecom Comments at 19-22.

[21] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, 37 FCC Rcd 13493 ¶¶ 65-66 (2022).

[22] *See, e.g.*, CTA Comments at 18-19; SEIA Comments at 3-6; TIA Comments at 24-26.

[23] *See* Foundation for Defense of Democracies Comments at 5.

[24] *See, e.g.*, AUVSI Comments at 3-4; CTA Comments at 28-34; CTIA Comments at 18-22; ITI Comments at 7-11; NEMA Comments at 2; SEIA Comments at 17-19; TIA Comments at 13-20.

[25] *See, e.g.*, CTA Comments at 34-36; CTIA Comments at 20; ITI Comments at 7; TIA Comments at 16-17; *2026 Minimum Elements for a Software Bill of Materials (SBOM)*, CISA et al., https://www.cisa.gov/sites/default/files/2026-07/2026_cisa_sbom_minimum_elements_508c.pdf (July 29, 2026).

record retention rules already require applicants to monitor their supply chains to avoid prohibited suppliers and enable the Commission to hold them accountable for these representations. If the Commission nevertheless decides to adopt SBOM/HBOM rules, it should take steps to enable compliance and reduce risks, such as requiring authorization holders to retain the relevant records and produce them upon request. Any new disclosure requirements should be strictly limited to entities on the Covered List and must provide for automatic, permanent confidential treatment for any disclosed information.[26]

***

CTA appreciates the Commission's work to refine the Covered List rules in light of new production location bans. The record clearly supports those steps, while cautioning against broader changes that would overhaul the existing equipment authorization program, which carefully balances promoting innovation and protecting consumers. Fortunately, the Commission can faithfully implement the Covered List without such measures. CTA welcomes further engagement with the Commission on this important effort.

Respectfully submitted,

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

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

[26] *See* CTA Comments at 32-35.