Before the
United States Federal Communications Commission
Washington, D.C.

In re 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

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

TABLE OF CONTENTS

The Computer & Communications Industry Association ("CCIA")[1] submits these reply comments in the ongoing *Third Report and Order and Third Further Notice of Proposed Rulemaking* (NPRM).[2]

Introduction

CCIA welcomes the opportunity to respond to the comments received in response to the Federal Communications Commission's ("Commission" or "FCC") NPRM. As noted in CCIA's initial comments, we support the Commission's efforts to protect national security. However, continued expansion of the Covered List and the rules surrounding it, without a clear nexus to a security concern, could have adverse outcomes for the U.S. economy and global leadership in new technologies.[3] In particular, the Commission should distinguish restrictions tied to identified entities or demonstrated national security risks from broad production-location rules that can reach manufacturing in allied and non-adversary jurisdictions. These reply comments address the following points raised in the docket:

- Entity-specific restrictions addressing identified national security risks should not be conflated with broad production-location restrictions that sweep in allied and non-adversary supply chains;
- Expansive "produced by" definitions, component restrictions, marketplace obligations, proactive HBOM/SBOM filings, revocation and pre-authorization reforms, and fixed authorization terms are inadvisable;

[1] CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at http://www.ccianet.org/members.

[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, Docket No. 21-232, FCC-26-50 (rel. July 23, 2026) (R&O or NPRM).

[3] Comments of the Computer & Communications Industry Association in Docket No. 21-232 (filed Sept. 8, 2026) ("Comments of CCIA").

- The Commission should reconsider or appropriately tailor numerous proposals to avoid harmful and unnecessary burdens on U.S. industry;
- Should additional supply chain safeguards be necessary, they should be targeted and workable.

I. Adoption of overbroad proposals would impede or curtail production across allied and non-adversary jurisdictions to the detriment of the U.S. economy and global technological leadership.

The Commission's production-location determinations for certain device sectors and proposed rules are not narrowly targeted at specific named foreign adversaries.[4] Continued adoption of these measures would establish broad country-of-origin restrictions that sweep in friendly trade partners and non-adversary global supply chains. This approach also fails to account for measures manufacturers employ to secure production facilities and protect intellectual property, trade secrets, and supply chains regardless of where those facilities are located. The Commission should avoid actions that promote creation of an overbroad, unworkable geographic dragnet that disproportionately impacts allied nations, harms domestic U.S. R&D, and imposes billions in unnecessary economic costs.

There is a stark mismatch between the NPRM's geographic reach and the actual market presence of equipment produced in foreign adversary countries.[5] Taking China as an example, in the customs line containing consumer routers subject to production-location rules, 98.9 percent of 2025 imports originated outside foreign-adversary jurisdictions, while China accounted for

[4] *See, e.g.* Comments of Foundation of Defense for Democracies in Docket No. 21-232 (filed Aug. 7, 2026) ("Comments of FDD") (framing proposals around preventing Chinese espionage, sabotage, and equipment from infiltrating U.S. networks); Comments of Digital Progress Institute in Docket No. 21-232 at 1-6 (filed Sept. 8, 2026) (asserting that "the national-security record supports action against China-based router manufacturers"); Comments of the Coalition for a Prosperous America in Docket No. 21-232 (focusing narrowly on the risks posed by Chinese optical transceivers) (filed Sept. 8, 2026).

[5] Trevor Wagener, *The Supply Chain Costs of the FCC's 2026 Covered List Regime*, Computer & Communications Industry Association Research Center (Sept. 2026), https://ccianet.org/research/reports/the-supply-chain-costs-of-the-fccs-2026-covered-list-regime/ ("CCIA Research Center Study").

just 1.1 percent.[6] Because the Commission's proposed rules penalize foreign production generally rather than focusing on foreign adversaries, the primary impact falls on products manufactured in allied nations like Japan, Germany, Canada, Mexico, and Taiwan, rather than China.[7]

Moreover, CCIA's economic modeling demonstrates that the broad geographic scope would create billions in excess costs compared to a standard strictly targeted at foreign adversaries. As currently applied, production-location restrictions would cost approximately $4.4 billion over five years. If the Commission were to limit current production-location restrictions strictly to foreign adversary jurisdictions (such as China), the five-year cost would fall to $0.1 billion. The comparison demonstrates that the geographic scope of the rule, rather than restrictions directed at foreign adversaries themselves, drives approximately $4.3 billion of the modeled five-year cost.[8] The Commission can substantially reduce those costs while preserving the core national security objective by distinguishing foreign-adversary jurisdictions from allied and other non-adversary trading partners.

II. Expansive "produced by" definitions would create substantial regulatory uncertainty and extend restrictions far beyond demonstrated national security risks.

CCIA opposes the Commission's proposed "totality of the circumstances" test and vague standards like "substantial responsibility" or "control over design," which introduce deep regulatory uncertainty. Additionally, CCIA warns against conflating entity-specific "produced by" rules with broad "produced in a foreign country" geographic dragnets. Furthermore, importing Buy American domestic-end-product cost thresholds as sought by FDD[9] into the equipment authorization regime would apply a procurement standard developed to advance domestic purchasing preferences to a regulatory program intended to mitigate national security

[6] *Id*.
[7] *See* Comments of CCIA at 11 (warning that the Commission's proposal to preclude any foreign manufacturer of a product on the Covered List from using SDoC would violate free trade agreements with allied partners).
[8] CCIA Research Center Study.
[9] Comments of FDD at 5.

risks. More broadly, applying production-location restrictions across components regardless of the jurisdiction in which they are produced generates approximately $4.3 billion in modeled excess costs over five years and imposes substantial costs on supply chains involving allied trading partners such as Japan, Germany, Canada, Mexico, and Taiwan without more closely targeting foreign-adversary risks.[10]

III. Expanded supply-chain documentation and re-certification would impose substantial costs without commensurate security benefits.

A. The FCC should decline mandatory, proactive HBOM/SBOM filings.

The Commission should reject calls to mandate proactive HBOM and SBOM submissions at the time of equipment authorization.[11] As numerous commenters recognize, applicants may not possess supply-chain information held exclusively by upstream suppliers.[12] If the Commission nevertheless requires submission of such documentation, it should distinguish between information reasonably available to an applicant and information held exclusively by independent suppliers, with appropriate safe harbors for applicants that reasonably rely in good faith on supplier-provided information.

Mandatory proactive HBOM/SBOM filing requirements would impose substantial financial burdens, risk commercial trade secret exposure, create cybersecurity vulnerabilities, and exacerbate the problems of the Commission's current Equipment Authorization System (EAS) database. CCIA Research Center estimates that requiring proactive HBOM/SBOM submissions at initial authorization would cost industry approximately $151 million annually, rising to as much as $265 million annually under the FCC's higher-end cost assumptions.[13] Additionally, storing granular component blueprints in centralized federal databases creates attractive targets for bad actors seeking competitive intelligence or opportunities for

[10] Comments of CCIA at 5; CCIA Research Center Study.
[11] Comments of FDD at 4; Comments of The Agricultural Drone Initiative in Docket No. 21-232 at 5 (filed Sept. 8, 2026) ("Comments of ADI").
[12] *See, e.g.*, Comments of Gatewell Group LLC in Docket No. 21-232 at 10 (filed Aug. 20, 2026) ("Comments of Gatewell").
[13] CCIA Research Center Study.

counterfeiting.[14] Finally, the Commission's current EAS database was not designed to securely process structured HBOM/SBOM data at this scale.[15] Mandating filings before deploying tested, secure, machine-readable API infrastructure would create significant compliance bottlenecks on top of existing security risks.[16]

Three very different regulatory approaches present themselves to the Commission: 1) requiring manufacturers to maintain supply-chain information internally; 2) requiring production of that information upon Commission request; and 3) requiring proactive filing of that information with every equipment authorization application. Even if the Commission concludes that applicants should maintain certain HBOM or SBOM information, that does not establish a need to routinely transmit sensitive supply-chain information to a centralized federal database. A targeted record-retention and production-on-request regime would substantially reduce cybersecurity, trade secret, and administrative concerns while preserving the Commission's ability to obtain relevant information when necessary. The FCC should, therefore, curtail this requirement to a subset of regulated entities subject to a Covered List designation supported by a national security determination.

B. The Commission should consider the costs and burdens inherent in multi-tier supply-chain accounting and physical verification proposals.

CCIA cautions against proposals to mandate multi-tier tracing across all components, which would impose substantial compliance burdens without a commensurate security benefit.[17] Enterprise IT and telecommunications equipment contain thousands of components from hundreds of suppliers across multiple tiers,[18] and requiring applicants to maintain complete

[14] Comments of CCIA at 8.
[15] *Id.* at 26.
[16] *Id.* at 25.
[17] *See, e.g.,* Comments of Modgud Laboratories LLC in Docket No. 21-232 at 1 (filed Aug. 31, 2026) ("Comments of Modgud") (arguing that self-declared bills of materials are insufficient to stop white-labeling and component evasions and proposing a mandatory three-tier assurance model with independent physical laboratory sampling and teardowns; Comments of Gatewell at 6-8 (recommending mandating a whole-device value calculation and a tiered supply-chain traversal rule that would require applicants to trace certain other components through direct suppliers to the entity that physically produced the component).
[18] Comments of CCIA at 6.

accounting across sub-tier producers would be extraordinarily difficult in complex global supply chains.[19] Furthermore, requiring country-of-origin and value tracking down to non-logic bearing passive parts (such as resistors, capacitors, and mechanical hardware) would yield no security benefit because non-logic parts cannot execute code or be manipulated remotely. Accordingly, component restrictions justified by national security purposes should be strictly limited to logic-bearing hardware (i.e., chips, processors, and programmable modules).

C. Mandatory re-certifications would divert resources away from actions to promote national security.

The Commission should preserve permissive-change pathways for software and firmware updates, which allow manufacturers to deploy security patches without unnecessary regulatory delay.[20] Proposals to require new equipment authorization for minor software or firmware updates would delay deployment of security patches while manufacturers await additional authorization, potentially extending remediation timelines from days to weeks.[21] This administrative paperwork would also divert engineering resources away from rapid vulnerability remediation, leaving American networks exposed to cyber threats. In contrast, making software/firmware permissive changes permanent for authorized equipment would save approximately $22 million per year while ensuring rapid deployment of critical security fixes.[22]

IV. Expansion of streamlined equipment authorization revocations beyond clear cases of willful misconduct or genuine emergencies would raise serious procedural and due process concerns.

Contrary to some arguments in the record, reliance on applicant disclosures and traditional administrative inquiries (such as Letters of Inquiry) would not lead to widespread instances of non-compliant entities delaying or evading FCC enforcement.[23] Thus, the

[19] *Id.*
[20] Comments of CCIA at 28-29.
[21] Comments of FDD at 5; Comments of ADI at 7.
[22] CCIA Research Center Study.
[23] Comments of Modgud at 3.

Commission should decline calls to establish a post-market enforcement framework where any physical discrepancy detected during lab sampling would automatically trigger an enforceable revocation event.[24] Streamlined or expedited revocation mechanisms should remain confined to clear cases of willful misconduct or genuine emergencies.[25] Where material facts are disputed or a potential violation involves a good-faith compliance issue, authorization holders should receive adequate notice, access to the evidence supporting the proposed action, and a meaningful opportunity to respond before an authorization is revoked.[26]

Moreover, the Commission should reject calls to rely on independent accredited laboratory teardown/sampling reports as actionable proof of non-compliance with FCC rules.[27] Any revocation process relying on third-party laboratory findings should provide the authorization holder timely access to the evidence on which the Commission proposes to rely and a meaningful opportunity to inspect, contest, or supplement that evidence before final agency action.

Finally, a physical discrepancy between the hardware and the filed HBOM should not automatically jeopardize a device's authorization.[28] Adoption of such a proposal would convert revocation authority into an automatic or mechanized process. The Commission's revocation procedures under Section 2.939 include express procedural safeguards essential to due process.[29] Automatically revoking previously compliant equipment due to subsequent Covered List updates or minor supply chain variations would sweep up lawfully deployed, active equipment in the market and severely chill domestic innovation.[30]

---

[24] *Id.* at 4.
[25] Comments of CCIA at 19.
[26] *Id.*
[27] Comments of Modgud at 4.
[28] *See* Comments of Modgud at 3 (contending that treating a discrepancy between the sampled hardware and the filed bill of materials as a defect attributable to the lot and to the authorization "is directly portable to the equipment authorization program").
[29] *See* 47 C.F.R. § 2.939(a)(4), (b); *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, ¶¶ 114–15 (2022) ("2022 Covered Equipment Order").
[30] Comments of CCIA at 19-20.

V. Fixed expiration terms on equipment authorizations would impose substantial costs and create significant regulatory uncertainty.

The Commission should decline to adopt a uniform automatic expiration date across all equipment authorizations.[31] Advocates for such proposals fail to recognize that the Commission already possesses explicit revocation authority under Section 2.939 to address equipment subsequently identified as a national security threat. Imposing rolling expiration dates based solely on the age of an authorization would therefore duplicate existing Commission authority without a demonstrated security benefit where the device's design and radio frequency (RF) characteristics have not materially changed.[32]

Additionally, applied to the roughly 233,000 equipment authorizations currently in commercial life, the Commission's proposed rolling 10-year term limits would impose approximately $47 million per year in additional administrative costs on industry. They would also create unresolved operational questions and potential market disruptions.[33] It remains unclear whether recertification would evaluate devices under rules in effect at original certification or under newly adopted rules.[34] The FCC has also provided no clarity on whether operating active, previously purchased devices in consumers' hands would suddenly become illegal. Further, retailers holding lawfully manufactured inventory not yet sold would face regulatory limbo.[35]

[31] Comments of FDD at 5 (arguing that periodic expirations allow the Commission to reevaluate older equipment against emerging national security risks).
[32] Comments of CCIA at 24.
[33] CCIA Research Center Study; Comments of CCIA at 24.
[34] *See id.* (requesting that the Commission provide a clear explanation of processes for renewal, including whether renewals would be based on the regulations at the time of original certification or would reflect rules in effect at the time of renewal).
[35] "Clarification would also need to be given as to, among other things, whether operation of devices that have been purchased or deployed could continue and what would happen to inventory of devices in the hand of retailers but not yet sold." *Id.*

VI. Restricting pre-authorization exceptions would undermine legitimate product testing and development.

The Commission should retain the existing pre-authorization importation allowance rather than reduce the per-model limit for testing, evaluation, and product development from 4,000 units to 40. A 40-unit limit would be insufficient for many forms of meaningful hardware and software evaluation, including RF validation across diverse environments, large-scale mesh networking testing, beta testing programs, internet service provider certifications, and statistical quality assurance.[36] These concerns are echoed throughout the record. The National Association of Manufacturers warns that reducing the allowance to 40 units would "significantly impair product development and testing."[37] TechNet similarly warns that a 40-unit limit "would upend legitimate trials without a corresponding benefit to national security,"[38] while the Consumer Technology Association explains that 40 units "cannot accommodate" customer acceptability and interoperability testing, among other development needs.[39]

In advanced robotics and UAS, physical hardware is an essential input into training and testing AI foundation models. Field testing complex systems across multiple facility types, operating conditions, and geographies requires test volumes well above 40 units.[40] Moreover, unless fewer than 1 in 20 programs need more than 40 units, the cap will cost industry well over $100 million per year.[41] Yet the record does not demonstrate that the existing 4,000-unit testing allowance has created a national security risk that would justify reducing the limit by 99 percent. Pushing import approvals into the proposed written-approval process under Section 2.1204(c)(2) merely shifts these costs into an unstandardized, untimed administrative queue.[42] Testing

[36] Comments of CCIA at 14.
[37] Comments of the National Association of Manufacturers in Docket No. 21-232 at 3 (filed Sept. 8, 2026) ("Comments of NAM").
[38] Comments of TechNet in Docket No. 21-232 at 5 (filed Sept. 8, 2026).
[39] Comments of Consumer Technology Association in Docket No. 21-232 at 8 (filed Sept. 8, 2026) ("Comments of CTA").
[40] *Id.*
[41] CCIA Research Center Study.
[42] *Id.*

exceptions must protect hardware for competitive teardowns, software development, and intellectual property evaluation, which keep American firms competitive.[43]

VII. Proposed e-commerce obligations would impose unworkable and unequal compliance burdens.

The Commission should not impose new point-of-sale display or verification obligations on online marketplaces without first addressing the technical and operational limitations that make those requirements impracticable at scale. Supporters of proposed mandates to display a device's FCC ID at the point of sale[44] or verify, rather than merely display, equipment authorization and compliance information[45] overlook basic technical, logistical, and operational realities of modern e-commerce. FCC IDs frequently appear on internal hardware labels, product packaging or via electronic labeling (e-labeling). Online marketplaces that do not take physical custody of inventory have no independent way to inspect or extract these IDs prior to listing.

Supporters of new requirements treat marketplace listings like small, static catalogs. But major platforms like Amazon and eBay host more than three billion listings, with over two billion representing used or consumer-to-consumer goods sold by hundreds of thousands of small businesses.[46] At minimum, the Commission should not impose independent verification obligations on online marketplaces until it has deployed a complete, reliable, and machine-readable database that allows platforms to perform those verifications at scale. The Commission cannot reasonably require marketplaces to verify information that its own systems do not make reliably and programmatically available. Once that infrastructure exists, any

[43] Comments of CCIA at 14.
[44] Comments of ADI at 2 (incorrectly describing requiring online marketplaces to display a device's FCC ID at the point of sale as a "de minimis obligation" that forces online retailers to declare what they are selling).
[45] Comments of Association for Uncrewed Vehicle Systems International in Docket No. 21-232 at 8 (filed Sept. 9, 2026) (supporting requirements that online marketplaces verify, rather than merely display, equipment authorization and compliance information).
[46] Comments of CCIA at 15; CCIA Notice of Ex Parte Communication, ET Docket No. 21-232 (July 14, 2026), https://www.fcc.gov/ecfs/search/search-filings/filing/26110017302.

marketplace obligations should be paired with a safe harbor for platforms that reasonably rely in good faith on Commission-maintained data.

Additionally, requiring online platforms to collect, verify, or display compliance data would create materially different compliance obligations based solely on the channel through which identical equipment is sold. Physical brick-and-mortar retailers are not required to independently validate or display these data points at the register, and the record does not identify a national security rationale for imposing substantially greater verification obligations when the same product is sold online. Finally, absent appropriate safe harbors, potentially significant liability for third-party compliance failures would incentivize platforms to engage in aggressive de-risking, which would result in marketplaces proactively removing broad categories of legitimate products from their sites. This compliance uncertainty ultimately harms consumers through reduced product selection and higher prices.

VIII. The Commission should decline to adopt proposals that would produce harms across a host of industries to the detriment of the public interest.

Comments from stakeholders across manufacturing, clean energy, communications, retail, event management, and consumer goods demonstrate that the operational consequences of the Commission's proposals extend well beyond the technology sector. Across these industries, commenters repeatedly urge the Commission to adopt targeted, risk-based requirements rather than broad mandates that would disrupt product development, supply chains, and lawful commerce.

A. The FCC should confine component restrictions strictly to logic-bearing hardware.

Like CCIA, major non-tech trade associations and industry coalitions urged the Commission to confine component prohibitions strictly to logic-bearing hardware and explicitly

exempt passive or non-logic-bearing components.[47] Some broadband stakeholders also underscore that broad component bans exceed statutory authority under the Secure Networks Act, advocating instead for a rebuttable presumption focused strictly on whether a component can process information, execute code, or affect RF emissions.[48]

B. The Commission should reject proactive HBOM/SBOM filings.

Several non-tech stakeholders similarly distinguish between maintaining supply-chain information and proactively filing that information with the Commission. These commenters warn that centralized submission of granular HBOMs/SBOMs could impose substantial administrative costs, expose trade secrets, and create cybersecurity risks.[49] Instead, one stakeholder recommends that the Commission only require parties to produce HBOMs and SBOMs on request "rather than to file them with every application," noting that a centralized federal repository of supply chain blueprints would itself become a "reconnaissance asset the Commission seeks to deny our adversaries."[50] CCIA recommends that the Commission reject

---

[47] *See*, *e.g.*, Comments of NAM at 2 (recommending that the FCC "exempt passive components, whose risk profile is not comparable to that of remotely exploitable hardware or software"); Comments of the National Electrical Manufacturers Association in Docket No. 21-232 at 4 (filed Sept. 8, 2026) ("Comments of NEMA") (urging the Commission to avoid imposing "unnecessary burdens on equipment or components that do not present [national security] risks" and to restrict rules to security-relevant logic-bearing parts); Comments of the Toy Association in Docket No. 21-232 at 4 (filed Sept. 8, 2026) (requesting that mandatory disclosures and bans "should not include components unrelated to the electronic function of a product or component such as screws, fasteners, and passive electrical components that would not be considered 'logic-bearing hardware', as they do not perform computing or processing functions").

[48] Comments of NTCA in Docket No. 21-232 at 3 (filed Sept. 8, 2026) (arguing that if the Commission "has reason to believe certain components pose a threat to national security or otherwise meet the criteria established by the Secure Networks Act, the Commission should provide a rebuttable presumption that allows the entity seeking equipment authorization to demonstrate "that the device incorporating such a component *does not* pose 'unacceptable risks to the national security of the United States or to the safety and security of United States persons'"); Comments of WISPA in Docket No. 21-232 at 3 (filed Sept. 8, 2026) (urging the Commission to "adopt a rebuttable presumption against authorizing devices that incorporate component parts that are produced by a Covered List entity, rather than outright prohibiting equipment authorizations for such devices").

[49] *See* Comments of NAM at 1 (warning that proactive filings "would transform equipment authorization into an expansive supply-chain reporting program whose costs would exceed its demonstrated security value and risk being infeasible," while failing to "protect trade secrets, source-code information, pricing, and third-party intellectual property from public disclosure"); Comments of Commercial Drone Alliance in Docket No. 21-232 at 2 (filed Sept. 8, 2026) ("Comments of CDA") (stating that mandatory HBOM/SBOM disclosures "would impose significant costs and delays on American UAS manufacturers, while providing little incremental value in advancing the Commission's national security objectives").

[50] Comments of Carnegie Endowment for International Peace in Docket No. 21-232 at 1 (filed Aug. 13, 2026).

proactive HBOM/SBOM filing requirements and instead permit manufacturers to maintain this information internally and produce it upon specific request from the Commission.

C. The Commission should preserve pre-authorization R&D, testing import caps, and tradeshow exemptions.

Non-tech stakeholders strongly endorse CCIA's defense of pre-authorization pathways under Sections 2.803, 2.805, and 2.1204 of the Commission's rules, asserting that controlled testing and demonstrations are essential for innovation.[51] Specifically, the National Association of Manufacturers (NAM) recommends that the Commission maintain the 4,000-unit testing import allowance, warning that slashing the limit to 40 units would "significantly impair product development and testing" across complex devices requiring RF validation in varied environments.[52]

D. The Commission should codify permanent permissive changes and reject 10-year authorization expirations.

Major non-tech trade associations align with CCIA in supporting permanent software/firmware permissive changes to enable rapid cybersecurity patching, while rejecting fixed expiration term limits on equipment authorizations.[53] NTCA specifically notes that term

---

[51] Comments of the Exhibitions and Conferences Alliance in Docket No. 21-232 at 2 (filed Sept. 8, 2026) (urging the FCC to "preserve the longstanding, carefully circumscribed rules that permit radiofrequency ('RF') devices that have not yet received equipment authorization to be imported, displayed, and operated temporarily for demonstrations at bona fide industry tradeshows and exhibitions); Comments of the Power Tool Institute in Docket No. 21-232 at 3 (filed Sept. 4, 2026) ("support[ing] allowing pre-authorization operation of RF devices… including trade-show demonstrations and pre-production evaluations of covered equipment"); Comments of the SAFE Alliance in Docket No. 21-232 at 8 (filed Sept. 8, 2026) (arguing for preservation of a "narrow safe harbor for non-operational trade-show display, clearly labeled pre-authorization demonstrations, controlled engineering testing and customer evaluation, and conditional sales arrangements where the device is not delivered for ordinary commercial use before authorization").

[52] Comments of NAM at 3.

[53] *See id.* at 4 (recommending against imposing "fixed term limits on equipment authorizations, and instead rely on revocation and material-change rules"); Comments of NEMA at 3 ("oppos[ing] the proposed term limits on equipment authorizations, and any restrictions on the continued operation of installed, lawfully authorized equipment"); Comments of NTCA at 7 ("urg[ing] the Commission to not place an expiration date on equipment authorizations").

limits would create a map of unsupported legacy products for bad actors to target and proposes instead that the Commission "allow the equipment to 'age out naturally.'"[54]

E. The Commission should uphold due process in revocation proceedings and maintain Supplier's Declaration of Conformity (SDoC) pathways.

Stakeholders across sectors mirror CCIA's position that administrative due process must be preserved during equipment revocation proceedings, and that non-covered equipment should not be stripped of SDoC eligibility.[55] The American Clean Power Association (ACP) and Solar Energy Industries Association (SEIA) urge that the Commission preserve written notice, an opportunity to respond and cure good-faith compliance issues, and formal due process under the APA for non-willful matters.[56]

IX. Tech industry commenters broadly support a targeted, risk-based supply chain security framework while differing on particular compliance mechanisms.

Comments from tech trade associations, equipment manufacturers, communications providers, and e-commerce platforms demonstrate broad support for a targeted, risk-based supply chain security framework. Although commenters differ on particular compliance mechanisms, substantial portions of the industry record caution against requirements that are overly broad, administratively burdensome, or disconnected from demonstrated national security risks.

Like CCIA, other tech trade associations argue that the Commission's authority under the Communications Act is tied to RF compliance and that national security restrictions must be

---

[54] Comments of NTCA at 7.

[55] *See* Comments of the American Clean Power Association in Docket No. 21-232 at 14 (filed Sept. 8, 2026) ("Comments of ACP") (recommending that "any streamlined revocation procedure the Commission adopts" include written notice, an opportunity to respond and cure good-faith compliance issues, and formal due process under the APA); Comments of Solar Energy Industries Association in Docket No. 21-232 at 27 (filed Sept. 8, 2026) ("Comments of SEIA") (mirroring the recommendations of ACP); Comments of CDA at 3 (warning that "[r]equiring certification for all devices in Covered List sectors would impose substantial additional costs, regulatory burdens, and delays on American UAS manufacturers, regardless of actual risk level, while offering little corresponding national security benefit").

[56] Comments of ACP and Comments of SEIA *supra* note 55.

strictly confined to logic-bearing hardware, explicitly excluding passive, non-RF, or commoditized parts.[57] Many of these stakeholders also raise concerns that proactive HBOM/SBOM filing requirements and 30-day update obligations would impose substantial administrative burdens, expose sensitive commercial information, and create cybersecurity risks.[58]

On slashing the testing importation cap and trade show and pre-authorization operating exemptions, other tech industry stakeholders align with CCIA's positions refuting the Commission's importation cap proposal and defending such exemptions.[59] On proposed e-commerce obligations, online marketplace stakeholders oppose forced verification of FCC IDs and SDoC data at the point of sale, citing the absence of a public SDoC database, the scale of e-commerce, and the risk of aggressive platform de-risking.[60]

---

[57] *See*, *e.g.*, Comments of the Information Technology Industry Council in Docket No. 21-232 at 11 (filed Sept. 8, 2026) ("Comments of ITI") (recommending that the Commission "treat logic-bearing hardware as the outer limit of any component prohibition"; Comments of Software & Information Industry Association in Docket No. 21-232 at 2 (filed Sept. 8, 2026) ("Comments of SIIA") (recommending that "the Commission preserve the Third Report and Order's focus on logic-bearing hardware components rather than extent prohibitions to passive parts"); Comments of TechNet at 5 (noting that "many components, such as passive electronics that perform no logic function, pose no meaningful risk no matter where or by whom they were made"); Comments of Mobile & Wireless Forum in Docket No. 21-232 at 11 (filed Sept. 8, 2026) ("Comments of MWF") (warning that "a categorical prohibition extending to non-RF components… would sweep far beyond national security objectives"); Comments of Japanese Electronics and Information Technology Industries Association in Docket No. 21-232 at 3 (filed Sept. 8, 2026) ("Comments of JEITA") (explaining that non-digital components that "have no logic functions and cannot be programmed have no capability to interfere with a device's communications, control, or cybersecurity… do not pose a risk to U.S. national security or to the safety and security of the American public").

[58] Comments of Telecommunications Industry Association in Docket No. 21-232 at 13 (filed Sept. 8, 2026) ("Comments of TIA"); Comments of ITI at 7; Comments of JEITA at 2; Comments of INCOMPAS in Docket No. 21-232 at 26 (filed Sept. 8, 2026); Comments of CTA at 29.

[59] *See* Comments of TechNet at 5 (explaining that "[c]utting the testing-and-evaluation limit to 40 units per model… would upend legitimate trials without a corresponding benefit to national security); Comments of CTA at 8 (warning that a 40-unit cap "cannot accommodate" customer acceptability and interoperability, among other needs); Comments of Association for Advancing Automation in Docket No. 21-232 at 8 (filed Sept. 8, 2026) ("Comments of A3") (explaining how elimination of the trade show exception "or reducing the number of devices that can be imported for display at industry trade shows would prevent exhibitors from displaying and demonstrating new and emerging technologies at U.S. events and trade shows before those products have received final FCC authorization or secured Conditional Approval") ; Comments of TIA at 28 (noting particular concern with the proposal to slash the testing-and-evaluation limit).

[60] Comments of eBay in Docket No. 21-232 at 8-9 (filed Sept. 8, 2026); Comments of INCOMPAS at 5; Comments of ITI at 14; Comments of CTA at 39.

Moreover, like CCIA, other tech trade associations strongly support codifying permanent Class I and II software/firmware permissive changes to allow rapid security patching without administrative delays, while opposing fixed ten year expiration terms on authorizations.[61] Numerous associations like CCIA also oppose eliminating Section 2.939(b) and streamlining non-willful revocations.[62] Furthermore, several stakeholders also support CCIA's proposed 30-day response period for non-willful revocation proceedings.[63] On SDoC, most tech industry stakeholders oppose universal registration across Covered List sectors.[64]

Conclusion

As stated in our comments to the Commission's NPRM, CCIA supports the goal of protecting the security and integrity of the nation's communications supply chain. That objective, however, is best served through targeted, risk-based measures that address demonstrated national security threats without imposing unnecessary costs, disrupting global supply chains, or undermining American innovation and technological leadership.

For the foregoing reasons, CCIA urges the Commission to preserve workable compliance pathways for manufacturers, suppliers, retailers, and online marketplaces. The record demonstrates substantial cross-industry concern regarding overbroad production-location restrictions, indiscriminate component tracing, centralized supply-chain disclosures, burdensome recertification and importation requirements, and compliance obligations that cannot be implemented using existing Commission infrastructure. The Commission should account for those concerns as it develops any final rules in this proceeding.

---

[61] *See*, *e.g.*, Comments of CTA at 40 (arguing that "Requiring Renewals of Equipment Authorization Diverts Resources from New Devices to Old Ones Without Materially Enhancing Compliance"); Comments of MWF at 41 (noting that "[m]any certified and SDoC devices remain in service well beyond ten years"); Comments of INCOMPAS at 67 (recommending that the FCC reject equipment authorization term limits).

[62] *See*, *e.g.*, Comments of SIIA at 8 (insisting that where material facts are disputed, grantees must receive supporting evidence and have "at least 30 days to respond rather than the 10 days proposed"); Comments of INCOMPAS at 6 (urging preservation of "adequate notice, an opportunity to cure, and meaningful hearing and review rights" in any expanded revocation procedure); Comments of ITI at 9-10 (mirroring INCOMPAS's recommendation).

[63] Comments of SIIA *supra* note 57.

[64] *See*, *e.g.*, Comments of INCOMPAS at 41; Comments of ITI at 12; Comments of TIA at 21.

Respectfully submitted,

Brian McMillan
Vice President, Head of U.S. Policy
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
bmcmillan@ccianet.org

Rachel Grey
Technology Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
rgrey@ccianet.org

September 28, 2026