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	Docket No. 21-232

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the *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* published in the Federal Register at 91 Fed. Reg. 51139 (Aug. 7, 2026), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments.

Introduction

CCIA welcomes the opportunity to respond to the Federal Communications Commission's ("Commission" or "FCC") *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program Third Report and Order* ("R&O") *and Third Further Notice of Proposed Rulemaking* ("NPRM"). While CCIA supports the Commission's mission to protect national security, the continued expansion of the Covered List and the rules surrounding it could have adverse outcomes for the U.S. economy.

[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.

The large economic costs of the FCC's proposed rules and recent related covered list actions warrant significantly more thorough economic analysis and consideration of less costly alternatives. The CCIA Research Center estimates[2] the rules adopted in the R&O would cost approximately $814 million over five years, which is nearly 1.7 times the Commission's $489 million cost estimate. The FCC's Covered List actions, specifically the production-location determinations for routers, power inverters, drones, and robots, which the Commission's cost analysis does not consider, add about $4.4 billion over five years in additional costs under CCIA's models. CCIA has not found any agency estimate of the costs of the production-location determinations against which to compare its estimates. The proposals in the NPRM would add approximately $2.4 billion over five years in additional costs in CCIA's models.

In addition to CCIA's economic concerns, the short period in which to respond to this NPRM did not provide adequate time for industry organizations including CCIA to coordinate substantive policy responses among their members to the more than 200 questions in the NPRM. CCIA and other associations requested an extension of time for this and other reasons, to which the Commission responded by only providing a seven-day extension for reply comments.[3] CCIA will continue to provide the Commission with additional information and analysis, but we remain concerned that the compressed schedule is poorly suited to a proceeding of this breadth and potential consequence for U.S. technological leadership and the health of the economy.

These comments, however, do not focus on CCIA's procedural concerns. Substantively, our comments focus on the following priorities:

- Distinguishing Covered Entities from Covered Sectors;

---

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

[3] Joint Request for Extension of Time of the Computer & Communications Industry Association et al., *In re* Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232 (F.C.C. filed Aug. 2026), https://ccianet.org/wp-content/uploads/securepdfs/2026/08/As-filed-Extension-Request-for-FCC-Secure-Equipment-3FNPRM.pdf; *In re* Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, Order, ET Docket No. 21-232, DA 26-888 (OET Aug. 2026), https://www.fcc.gov/document/oet-grants-joint-petitioners-seven-day-extension-reply-comments.

- Rejecting Overbroad "Produced By" and Supply Chain Accounting Mandates;
- Limiting Component Restrictions to Logic-Bearing Hardware;
- Opposing Proactive Hardware and Software Bills of Materials (HBOMs/SBOMs) Filings and Rolling Updates;
- Protecting Domestic Hardware R&D and Pre-Authorization Exceptions;
- Ensuring Feasibility and Safe Harbors for Online Marketplaces;
- Upholding Administrative Due Process in Revocation Proceedings; and
- Rejecting Arbitrary Term Limits and Overbroad Origin Definitions.

We discuss these priorities in the response below.

I. CCIA supports the Commission's proposal to bifurcate the Covered List to the extent that it provides clarity for understanding obligations and potential enforcement, but requests more information on potential rules that would apply only to the production-location-based category and to any device in a "Covered List sector."[4]

CCIA does not object in principle to the administrative act of bifurcating the Covered List into producer/provider-based and production-location categories, but we are concerned about how the production-location-based rules may apply. We urge the FCC to maintain a strict regulatory division between "entity-specific" and "location-specific" rules to avoid creating an unworkable country-of-origin dragnet. Specifically, CCIA opposes overbroad rule changes for sectors already subject to production-location-based Covered List determinations (e.g., UAS, advanced robots, routers, and power inverters). While we recognize the Commission's authority to protect national security, sweeping regulatory changes—specifically, converting self-declaration pathways to mandatory certification and extending geographic restrictions down to individual components—could significantly disrupt global supply chains and impede American

[4] *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program* Third Report and Order and Further Notice of Proposed Rulemaking ("Third R&O and FNPRM") at ¶ 129, FCC 26-50, ET Docket No. 21-232 (released July 23, 2026), https://docs.fcc.gov/public/attachments/FCC-26-50A1.pdf.

hardware R&D, particularly when other methods for ensuring security already apply (e.g., FAA Part 135 manufacturer-operator certification).[5]

CCIA further recommends eliminating the general reference in the rules to the "Covered List" and instead distinguishing between "Covered Entities" and "Covered Sectors." Such a distinction would promote greater regulatory clarity, as rules governing Covered Entities are often prohibitory, whereas those governing Covered Sectors are restrictive (but not outright prohibitive).

Finally, as the Commission considers adding more potential technological sectors into the Covered List, it must be done with industry input. As defined herein, the impacts of broad categorization in the Covered List to the U.S. supply chain and economy can be detrimental to U.S. leadership in technology. CCIA remains concerned about the lack of specificity that has been provided regarding national security threats for production facilities located outside the United States. Industry has strong incentives to adhere to stringent security practices to prevent leaks of new technologies, as well as theft of trade secrets and intellectual property (IP). Sharing more information about perceived national security threats could help industry harden their supply chains against the perceived potential harms underlying the proposed bans. In short, there are balanced approaches to ensuring national security while continuing to grow a globally competitive market, but these approaches require industry input.

II. White Labeling[6]

A. CCIA believes that codification of a definition of "produced by" could improve regulatory certainty, but cautions the Commission against implementing a definition that is overbroad, vague, and functionally unworkable.[7]

CCIA appreciates the Commission's intention to codify a definition of "produced by" to

[5] FAA Part 135 certified manufacturer-operators design, manufacture, and assemble their UAS, control UAS operations, and manage all software/firmware updates, thereby mitigating the national security risk associated with such UAS.

[6] Third R&O and FNPRM at ¶¶ 130-138.

[7] *See id.* at ¶ 130 ("seek[ing] comment on how and whether the phrase "produced by" in specific determinations as reflected on the Covered List should be interpreted").

improve regulatory certainty. This intention appears to contradict the Commission's determination in the R&O, in which the Commission "clarif[ies]... that the term "produced by" continues to be evaluated under the totality of the circumstances."[8] CCIA reiterates its concern, as addressed in its July 14 ex parte letter in response to the R&O,[9] that the Commission's determination incorporates vague factors such as having "substantial responsibility" or "control over design, development, manufacture, or assembly."[10] This standard will create substantial uncertainty for online marketplaces and retail distributors.

We recommend, instead, that the Commission adopt a clear framework grounded in industry best practices to prevent inconsistent enforcement and limit retroactive liability. This definition should distinguish between direct production relationships and incidental, downstream suppliers. Additionally, it should include clear, objective boundaries rather than a "totality of circumstances" standard that risks imposing unwarranted liability on applicants.

B. While excluding design entirely from the definition of "produced by" is not necessarily warranted, CCIA recommends that the Commission include a narrower, more qualified definition of "design involvement."[11]

CCIA is concerned that an open-ended inclusion of design in the definition of "produced by" would sweep in standard, low-risk industry practices (e.g., licensing IP or providing generic reference designs). Instead, we propose that "design involvement" have strict boundaries to limit "producer" status to entities with active, material control over a device's final specifications.

---

[8] *Id.* at ¶ 13.
[9] Comput. & Commc'ns Indus. Ass'n, Notice of Ex Parte Communication, ET Docket No. 21-232 (July 14, 2026).
[10] *Id*.
[11] *See* Third R&O and FNPRM at ¶ 134 ("seek[ing] comment on whether, the extent to which, and how design involvement should be incorporated into the definition of "produced by").

C. CCIA strongly opposes any requirement for applicants to submit a written, signed list of "any and all" entities that produced a device, as compliance with such a requirement would be practically impossible and only burden good actors.[12]

Requiring an absolute accounting of every upstream entity across multi-tier global supply chains is technically unworkable, legally hazardous, and disproportionate to actual national security risks. Modern enterprise IT and computing hardware contains thousands of components from hundreds of suppliers across multiple tiers. Equipment applicants rarely have direct commercial relationships or contractual visibility into lower-tier component makers and raw-material producers. Additionally, such a requirement would create an unreasonable standard of strict liability. Because supplier relationships constantly shift due to parts availability and second-sourcing, an applicant could inadvertently commit a certification violation—one that may not pose the kind of national security risk the Commission seeks to prevent—despite acting in good faith.

If the Commission retains a producer disclosure requirement, such a requirement must limit the scope to direct/material relationships (i.e., Tier 1 manufacturers, final assembly entities, or entities with direct, material decision-making control over device-specific design and production) and adopt a "knowledge" or "reasonable due diligence" standard. Adopting such a standard would mitigate the risk of facing strict liability for omissions in lower supply-chain tiers. Moreover, the Commission should, consistent with its approach in the R&O,[13] exclude from this requirement suppliers of passive, commoditized, or non-logic-bearing components.

III. CCIA strongly opposes the Commission's proposal to require applicants for equipment authorization to submit a written and signed HBOM and SBOM at the time of application for certification and provide updates of any changes.[14]

---

[12] *See id*. at ¶ 135 ("seek[ing] comment on whether to adopt a requirement that an applicant for equipment authorization provide a written and signed list of any and all entities that produced the device for which equipment authorization is sought").

[13] *See id.* at ¶ 20 (explaining that the Commission, "[g]iven the lack of support in the current record," opted against adopting "broader proposals to ban equipment authorizations for equipment incorporating components where there is not a nexus to a specific national security determination resulting in additions to the Covered List").

[14] Third R&O and FNPRM at ¶ 142.

While companies may be in the practice of maintaining HBOMs and SBOMs for cybersecurity and vulnerability management, CCIA is concerned that forcing proactive submission into the equipment authorization process will create overbroad, unworkable, and highly burdensome requirements that will ultimately risk exposing highly sensitive commercial trade secrets. Even more burdensome and unworkable, the Commission's proposal to require disclosure of each component, the location of each component's production, and the percentage of component value associated with each production location would not yield any tangible national security benefit, as many components of the devices in question have no bearing on national security.[15]

The CCIA Research Center estimates the HBOM/SBOM submission requirement at approximately $151 million per year across 26,545 annual original equipment grants.[16] This estimate uses half of the Commission's own anchors of up to $10,000 per device and under $5,000 per software program; at those ceilings the estimate is approximately $265 million.[17] The 30-day update obligation,[18] which would be both commercially and operationally disruptive, adds approximately $320 million per year, as it attaches to every material change across all authorizations on file.[19]

Should the Commission nevertheless proceed in adopting this economically and administratively burdensome mandate, CCIA urges limiting the requirement to Covered List sectors only and exempting trusted classes of equipment[20] (e.g., the Blue UAS Cleared List, Part 135 Carriers, Conditional Approval recipients, or Buy American-compliant manufacturers).[21]

---

[15] *Id.* at ¶ 142.

[16] CCIA Research Center Study, supra note 2.

[17] *Id.*

[18] Third R&O and FNPRM at ¶ 142.

[19] CCIA Research Center Study, supra note 2.

[20] CCIA believes the Commission should also consider whether other trusted classes of equipment or manufacturers might warrant an exception from these onerous obligations.

[21] *See* Third R&O and FNPRM at ¶ 144 (seeking comment on whether the Commission should "limit the HBOM and SBOM requirements to equipment authorizations for devices in a Covered List sector or a narrower subset of applicants" and whether there are "classes of trusted UAS or UAS critical components that should be exempt from such requirements, such as equipment included on the Defense Contract Management Agency's Blue UAS Cleared List, or for entities who are recipients of Conditional Approvals, manufacturers that satisfy the Buy American standard").

Limiting HBOM/SBOM requirements to devices in Covered List sectors would better tailor the requirement to address national security risks without imposing undue burdens on equipment devoid of national security concerns. The Commission should strictly limit this requirement to critical, security-relevant components rather than the entire device.[22] A universal, blanket mandate to track every single part of a device, as noted previously in this response, is technically unworkable and economically disproportionate, especially since the Commission has failed to provide an explanation of how this mandate yields any tangible national security benefit. The Commission should also, as suggested above, rethink requiring equipment grantees to update HBOM and SBOM submissions within 30 days of any material change.[23]

Furthermore, the Commission should not implement any HBOM/SBOM submission requirements without finalizing specific legal and procedural guardrails. At a minimum, any HBOM or SBOM filings should receive automatic confidential treatment and be protected from public disclosure, including through the Commission's public-inspection procedures or FOIA, given the sensitive information such filings would reveal regarding product architecture, supplier relationships, sourcing strategies, and component pricing. The filing systems should be protected by appropriate levels of cybersecurity protection to prevent bad actors from obtaining competitively sensitive information, which could be used for anti-competitive or even counterfeiting activities.

IV. Software and Other Components Produced by Covered List Entities[24]

A. CCIA believes that the Commission lacks both a clear national security and statutory basis for its proposal to extend prohibitions against authorizing devices incorporating any component produced by a Covered List entity.[25]

The FCC's authority under the Communications Act is traditionally tied to its radio-frequency (RF) compliance function. Therefore, extending prohibitions to non-RF, passive

[22] *See id.* at ¶ 145 (seeking comment on whether the Commission "should limit the HBOM/SBOM requirement to certain components").
[23] *Id.* at ¶ 142.
[24] *Id.* at ¶¶ 147-152.
[25] *Id.* at ¶ 148.

components lacks both a sound national security justification and a clear statutory basis. In contrast, the Commission drew the correct regulatory line in its R&O by limiting component restrictions to logic-bearing hardware (e.g., chips, processors, or modules capable of executing code or processing data).[26] Extending bans beyond the line drawn in the R&O to every non-RF would stifle American innovation without any concomitant enhancement to national security. A sound, risk-based national security policy must distinguish between components that can be manipulated by an adversary and those that cannot.

Importantly, the Commission has not provided a cost estimate for this proposed extension to its rules. The CCIA Research Center estimates the adopted logic-bearing prohibition alone would cost approximately $63 million per year.[27] The "any component proposal" would reach a population that is difficult to gauge at present but presumably could be far larger.

Rather than implementing such an overly broad prohibition, CCIA recommends that the Commission adopt a highly targeted, risk-based framework that focuses on plausible attack vectors, applies the compliance test to the security-relevant component itself, and leverages standard industry practices and established federal cybersecurity frameworks. If the Commission does proceed to adopt this prohibition, notwithstanding its lack of a nexus to a clear national security threat and lack of statutory basis to do so, it should establish a rebuttable presumption against authorization with a "preponderance of the evidence" standard.[28]

B. In considering how to address software/firmware-related risks, CCIA urges the Commission to distinguish between genuine software security controls and burdensome, administrative paperwork that could actually delay critical security patches.[29]

To address software and firmware-related security risks, CCIA recommends that the Commission take a highly targeted, risk-based approach that focuses exclusively on logic-

[26] *Id.* at ¶ 13.
[27] CCIA Research Center Study, supra note 2.
[28] Third R&O and FNPRM at ¶ 149.
[29] *See id.* at ¶ 150 ("seek[ing] comment on how software and/or firmware produced or provided by a Covered List entity, if incorporated into another device, raises unacceptable national security risks").

controlling elements. We support the Commission's current approach, which is to focus on logic-bearing hardware (i.e., chips, processors, and modules capable of executing code or processing data), as these programmable parts are the most plausible vectors for malicious code execution or remote manipulation.

In contrast, CCIA objects to the Commission's proposal to require updated SBOM submissions within 30 days of a material change. Imposing a recurring regulatory filing obligation tied to software changes would create unnecessary administrative burdens and could divert resources from the rapid development and deployment of critical security fixes.[30]

As a potential alternative to requiring submission of complex SBOMs with every product application, the Commission could consider requiring manufacturers to maintain a current internal SBOM and produce it only upon specific request from the FCC. However, as discussed previously here, should the Commission mandate submission of SBOM materials, the requirement should be strictly limited to equipment operating in Covered List sectors and not applied broadly to the entire universe of RF-authorized devices.

V. Requiring Certification for Devices in Covered List Sectors[31]

A. CCIA strongly opposes the Commission's proposal to amend 47 CFR § 2.907(c) to require certification of products that would otherwise be eligible for less burdensome procedures (including SDoC), but for their inclusion in Covered List sectors.[32]

CCIA generally opposes rules that would put specific imported products, other than those produced by an identified, untrustworthy supplier, at a competitive disadvantage relative to domestically produced products—particularly when the definition of "domestically-produced" is so stringent as to preclude broad swaths of equipment that rely on parts or components produced outside the United States from benefiting from non-discriminatory treatment. This issue is

[30] *Id.* at ¶ 142.
[31] *Id.* at ¶¶ 153-158.
[32] *Id.* at ¶ 154.

already in play with respect to routers, UAS, advanced robotic devices, and power inverters, which are subject to import prohibitions solely on the basis that they are manufactured abroad (untethered to any specific, discernible security risk and overlooking the strong incentives of industry participants to ensure that their manufacturing facilities, wherever located, are secure).

Manufacturers in some cases have been able to obtain conditional approvals for importation, but this procedure remains premised on disparate treatment that discriminates on the basis of foreign manufacture. It also remains cloaked in secrecy, with no clear criteria shared about how decisions about conditional approvals are being made or whether similarly-situated competitors are being subject to differential treatment. Proposals in the current NPRM would exacerbate these problems. For example, the proposed amendments to § 2.907 preclude any foreign manufacturer of a product on the covered list from using SDoC where that procedure is available to a domestic manufacturer. This arbitrarily puts certain classes of products at a distinct disadvantage, given the cost and efficiency benefits SDoC confers.

Not only does this approach violate the core obligation of national treatment integral to the World Trade Organization (WTO) and all free trade agreements, but it provides no discernable benefits with respect to national security. There is no obvious reason why a product manufactured in Japan, Germany, Canada, Mexico, or Taiwan should not be able to use SDoC if a domestic manufacturer could benefit from the process to obtain regulatory authorization for a similar product. Indeed, both devices assembled on U.S. soil could use the exact same components as the one assembled abroad but need to pursue entirely different paths to obtain authorization. Given the absence of a discernible security rationale, such disparate treatment would invite a challenge from trade partners that the Commission would have little basis of successfully defending. At a minimum, the Commission should limit this proposal to products produced in foreign adversarial countries where there has been an identified national security threat.[33]

[33] *See id.* at ¶ 154 (seeking comment on whether the proposed requirements "[s]hould… only apply to Covered List sector equipment produced in foreign adversary countries").

For the product categories currently subject to production-location restrictions, limiting those restrictions to equipment produced in foreign adversary jurisdictions identified under 15 C.F.R. § 791.4 (formerly § 7.4), while retaining existing producer-based exclusions, would cost approximately $0.1 billion over five years, compared with approximately $4.4 billion under the requirements as currently applied to routers, power inverters, drones, and advanced robotic devices, resulting in approximately $4.3 billion in modeled savings. These estimates apply to the product categories currently subject to production-location restrictions. Expanding a production-location restriction to additional categories of equipment would substantially increase the associated costs. About 98.9 percent of 2025 imports in the customs line containing consumer routers originated outside those jurisdictions, with China coming in at just 1.1 percent. The certification proposal itself would cost about $400 million per year on the Commission's own 10,000 to 100,000 device range.[34]

Considering quantifiable benefits is also useful in evaluating the relevant cost-benefit tradeoff. For example, even if a non-adversary standard retained just 70 percent of the domestic standard's security effectiveness, the domestic standard would need roughly $14.4 billion in five-year security benefits to justify its additional costs. The largest figure implied by the Commission's cited loss estimates and a one-percent prevention rate is $11.8 billion. Thus, even under the Commission's own assumptions, the record does not demonstrate that the domestic standard's incremental costs are justified. As the assumed effectiveness of the non-adversary standard approaches that of the domestic standard, the required incremental benefit rises further to $21.7 billion at 80 percent effectiveness and $43.3 billion at 90 percent.[35]

The Commission should also recognize that production in non-adversary jurisdictions under 15 CFR § 791.4 (formerly § 7.4) does not present the same national security concerns as production in foreign adversary countries. Even in cases of production in foreign adversary countries, the Commission's analysis ignores the incentives of market participants to secure their facilities against breaches that could lead to theft of trade secrets or intellectual property. Indeed, it has not been demonstrated that the national security threats that the production-based

[34] CCIA Research Center Study, supra note 2.
[35] *Id.*

exclusions are purported to quell are tied to site of manufacture at all. At a minimum, where the Commission nevertheless imposes production-location-based restrictions or conditions eligibility for Conditional Approval on supply-chain changes, it should permit reasonable reliance on non-adversary country sourcing rather than effectively requiring complete domestic onshoring. It also should provide greater transparency into its processes to ensure fair and non-discriminatory treatment of applicants. Such an approach would better reflect the realities of global technology supply chains while preserving the Commission's ability to target genuine national security risks.

B. CCIA strongly opposes the Commission's proposal to amend § 2.911 to require equipment-authorization applicants to submit additional disclosures as part of the certification process.[36]

In addition to being burdensome and in most cases lacking any material relevance to security issues, depending on how granular the requirements are, compliance with this proposal may simply not be feasible. At a minimum, such documentary requirements should only apply to materially relevant components, such as logic-bearing hardware and related software, rather than all components of covered communications equipment.

VI. CCIA strongly opposes the Commission's proposed dramatic narrowing of importation exceptions under 47 CFR § 2.1204 of its rules, as this would be practically unworkable, severely chill American R&D, and offer no actual national security benefits.[37]

CCIA opposes the Commission's proposals under § 2.1204 to narrow importation exceptions, particularly the proposal to slash the per-model importation limit for testing, evaluation, and product development from 4,000 units to 40 units, which would severely cripple hardware development.[38] We urge the Commission to maintain the current 4,000-unit importation limit.

[36] Third R&O and FNPRM at ¶ 157.
[37] *Id.* at ¶ 159.
[38] *Id.* at ¶ 161.

The proposed 40-unit cap is catastrophically low for meaningful product evaluation and would severely hamper innovation. Specifically, the proposed cap would be insufficient for, among other things, RF performance validation across diverse home environments, mesh networking performance at scale, beta testing programs, internet service provider certification testing, and quality assurance with statistical significance. A 40-unit cap is also insufficient for genuine product evaluation of complex robotics systems that require field testing across multiple facility types, operating conditions, and geographies. For bona fide R&D, robotics programs need to import units at volumes well above 40-units. Ultimately, such a cap would be incompatible with software testing at scale and would run counter to promotion of American global leadership in development of robotics.

The Equipment Authorization system records indicate 26,545 original grants in 2025 from 10,440 applicants. For the cap to cost industry less than $100 million per year, fewer than one program in 20 could need more than 40 units. The written-approval route in proposed § 2.1204(c)(2) relocates that cost into an unstandardized, untimed queue.[39]

The Commission should also clarify that the product-development and testing exception encompasses the use of imported hardware for competitive assessment (e.g., teardowns), software development, AI-model testing and training, and related research activities. In advanced robotics, physical hardware is itself an essential input into the development and testing of robotics foundation models. Restricting access to such hardware would therefore impair not merely hardware development, but U.S. development of the software and AI systems that operate across diverse robotic form factors. Furthermore, allowing for importation of hardware for teardown purposes helps American companies remain competitive and investigate potential IP breaches by bad actors.

[39]CCIA Research Center Study, supra note 2.

VII. Marketing Under 47 CFR § 2.803[40]

CCIA warns that many of the Commission's proposals to further restrict the marketing and operation of Covered List equipment within the United States are overbroad, retroactive, and would cause massive disruptions to both consumers and enterprise infrastructure.

A. CCIA strongly opposes the Commission's proposal to require online marketplaces to verify that FCC IDs and SDoC data match products.[41]

Requiring online marketplaces to collect, verify, and display SDoC compliance information statements or unique SDoC registration numbers at the online point of sale is an unworkable technical hurdle. Unlike FCC-certified equipment, there is no public or centralized SDoC database against which marketplaces could verify compliance information. This proposal would therefore effectively require marketplaces to verify information that cannot be independently validated.[42] The Commission should also avoid imposing obligations on online marketplaces that exceed those applicable to brick-and-mortar retailers. Requiring online marketplaces to independently collect, verify, or prominently display compliance information that physical retailers are not required to validate would create an unjustified regulatory disparity based solely on the method through which a product is sold, leading to a discriminatory result.

A requirement that online marketplaces display FCC IDs also ignores critical technical and logistical realities.[43] FCC IDs may appear on the device itself, its packaging, or through electronic labeling, and therefore may not be readily available to a marketplace that does not take physical custody of the product. Even where a marketplace does take physical custody, identifying and displaying the FCC ID for each listing could require additional manual processes that are difficult to implement at scale. These limitations are further exacerbated by the scale of modern e-commerce, with marketplaces such as eBay and Amazon alone hosting more than three

[40] Third R&O and FNPRM at ¶¶ 168-176.
[41] *Id.* at ¶ 168.
[42] *See* Comput. & Commc'ns Indus. Ass'n, Notice of Ex Parte Communication, ET Docket No. 21-232 (July 14, 2026), https://www.fcc.gov/ecfs/search/search-filings/filing/26110017302.
[43] CCIA is supportive of e-labeling and is not calling for additional packaging requirements, which would undermine the Commission's "Delete" efforts by adding regulatory burden.

billion listings from independent sellers. Of those listings, over two billion listings are for used and consumer-to-consumer goods.[44] This does not even account for other online marketplaces.

In the R&O, in which the Commission clarified that "[o]nline marketplaces that "market" unauthorized devices are subject to enforcement,"[45] the FCC also "acknowledge[d] the limits of the current available tools to help online marketplaces achieve compliance, including requirements to ensure that FCC IDs are not only valid but are accurate and match the product listings of the marketed equipment."[46] Responding to these concerns, the Commission claimed it made "reasonable edits… to the specific FCC ID display requirements" by, among other things, "further direct[ing] OET to work with the Enforcement Bureau (EB) and the Office of the Chief Information Officer (OCIO) as appropriate to modernize and update EAS as expeditiously as possible."[47] It also "direct[ed] OET to engage with online marketplaces to address technical improvements and updates related to the equipment authorization database, available application programming interfaces (APIs), and machine-readable data resources that support compliance monitoring and help prevent unauthorized marketing."[48]

The Commission's analysis contains the incorrect assumption that the problem has been resolved, as footnote 247 assigns the same $191,333 implementation cost to the largest marketplace and the fifteen-hundredth, despite no doubt enormous differences in catalog size and overhead. This is a deeply implausible cost assumption.

While CCIA appreciates the Commission's efforts to acknowledge its concerns, we find the response, unfortunately, to be vague and unworkable. CCIA further urges the FCC to rethink its rejection of requests for a safe harbor or knowledge requirement for the imposition of liability for online marketplace marketing.[49] Even if the Commission, as it claims, "is unlikely to pursue enforcement action against an online marketplace that undertakes reasonable due diligence to

---

[44] *See* Comput. & Commc'ns Indus. Ass'n, Notice of Ex Parte Communication, ET Docket No. 21-232 (July 14, 2026), https://www.fcc.gov/ecfs/search/search-filings/filing/26110017302.
[45] Third R&O and FNPRM at ¶ 55.
[46] *Id.* at ¶ 59.
[47] *Id.* at ¶ 60.
[48] *Id.*
[49] *Id.* at ¶ 61.

verify the device being offered for sale may be validly marketed under section 2.803(a),"[50] CCIA is concerned about capricious and unpredictable enforcement. For these reasons, we urge the FCC against adopting such a requirement.

The R&O does not define a single violation for a marketplace listing. Specifications range from one continuing violation at $188,491 to a per-model calculation that reached $34.9 million in a 285-model case.[51] In ASUSTeK (2024), the Commission said it "may change" to a per unit marketed methodology.[52] The uncertainty regarding potential enforcement costs may push impacted companies toward an aggressive de-risking regarding relevant products, which could have significant impacts on consumers. Uncertainty about enforcement exposure is likely to push marketplaces toward aggressive de-risking of the affected categories, an effect documented empirically for intermediaries under liability regimes,[53] predicted by the economics of compliance with uncertain standards.[54] The cost falls on consumers as a narrower assortment and higher prices.

B. CCIA strongly opposes the Commission's proposed narrowing of pre-authorization marketing and operating exceptions, such as those under § 2.803, for devices within Covered List sectors.[55]

The § 2.803 pre-authorization marketing and operating exceptions are essential for American product development, product launches, and collaborative feedback. These exceptions serve a fundamentally different purpose than the Covered List—supporting domestic R&D rather than commercial sales—and restricting them would paralyze product development and trade

---

[50] *Id.*

[51] *See* 47 C.F.R. § 1.80(b)(10); *C.T.S. Technology Co., Limited*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 8107, 8111–12 ¶¶ 12–14 (2014).

[52] *ASUSTeK Computer Inc.*, Notice of Apparent Liability for Forfeiture, FCC 24-69, ¶ 28 (2024).

[53] Daphne Keller, *Empirical Evidence of Over-Removal by Internet Companies Under Intermediary Liability Laws: An Updated List*, Stanford CIS (Feb. 2021), https://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws; *See also* Jennifer Urban, Joe Karaganis, and Brianna Schofield, *Notice and Takedown in Everyday Practice* (UC Berkeley/Columbia, 2017).

[54] Richard Craswell and John E. Calfee, *Deterrence and Uncertain Legal Standards*, 2 J.L. Econ. & Org. 279 (1986); *See also* Calfee and Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 Va. L. Rev. 965 (1984).

[55] Third R&O and FNPRM at ¶ 169.

engagement. Therefore, the proposed restriction would undermine American innovation and yield no national security benefit.

C. CCIA strongly objects to proactive marketing warnings and recommends that the Commission instead retain its existing, already sufficient disclosures.

The Commission's proposal to establish a new registration database to capture product identity is unnecessary and redundant, as this information is already collected.[56] Under § 2.1077, manufacturers must already complete a compliance information statement that identifies the responsible party, product name, and model number. Unless the Commission can demonstrate an incremental national security or public safety benefit to requiring a new registration database, it is unclear why such a database would be warranted.

D. CCIA opposes the Commission's proposal to require a warning for certain RF devices at the point of sale.[57]

While CCIA does not support the Commission's pursuit of overly broad marketing mandates, if it goes down this route, it should implement a programmatic, database-driven approach for point-of-sale warnings. This means identifying the devices that would potentially be subject to these mandates during the equipment authorization process and reflect that requirement as a structured data field in the OET EAS database.[58] This would allow online platforms to ingest the requirement via bulk API and display the required warnings programmatically to consumers before purchase. Should the Commission move forward with this requirement, it should permit machine-readable or clickable disclosures rather than requiring raw FCC identification information to occupy limited user-interface space on every relevant online surface.

---

[56] *See id.* at ¶ 172 (contemplating processes that could be implemented "to identify the marketing of authorized, limited, and revoked Covered List equipment that is being marketed within the United States").
[57] *Id.* at ¶ 174.
[58] *Id.*

VIII. CCIA believes that the Commission's proposal to extend the voluntary FCC logo to certified devices is not necessary, as certified devices already display the FCC ID.[59]

Additional logo mandates are redundant and provide no incremental compliance or traceability benefit. The Commission's most recent ruling on display of the FCC logo came in 2017, when the agency under the leadership of Chairman Ajit Pai determined it was no longer mandatory for SDoC devices. Adopting proposals in the NPRM would create confusion, with certified devices potentially being required to display both the FCC logo and an FCC ID, and with the Commission resurrecting a formerly deleted requirement for devices eligible for SDoC. The result would be a marketplace of different vintages, each marked in a legal way based on their time of authorization, with no consistency or indication that consumers even know what the FCC logo means. The issue will only be compounded with the addition of yet another logo on some devices—the U.S. Cyber Trust Mark.

CCIA opposes subjecting low-risk equipment to intrusive, burdensome premarket labeling or filing mandates that disrupt routine commercial deployments. Instead, the Commission should retain its current distinction between higher-risk intentional radiators and lower-risk equipment (e.g., IT hardware, digital apparatus, and non-intentional radiators) and should change requirements for display of logos. Rather, CCIA urges the Commission to continue following the direction of Congress in the E-Label Act pursuing electronic labels as sufficient and a preferred alternative to physical markings.

IX. CCIA opposes the Commission's proposed removal of § 2.939(b) and streamlining non-willful equipment-authorization revocations, as this would severely undermine grantees' due process rights under the Administrative Procedure Act (APA).[60]

Streamlined revocation mechanisms must remain strictly confined to clear, undisputed willful misconduct or genuine emergencies, rather than applied categorically to all revocations involving covered equipment. Any revocation involving non-willful issues, compliance misunderstandings, or disputed facts must undergo standard, full due process. Moreover,

[59] *Id.* at ¶ 178.
[60] *Id.* at ¶ 184.

lowering the legal bar for revocation would create due process concerns as well as severe regulatory uncertainty, chill innovation, and risk sweeping up equipment that is already actively deployed in the market.

Specifically, the Commission's proposed 10-day response window for expedited revocations is insufficient for resolving complex, multi-tier supply chain disputes. The Commission should expand the response window to at least 30 days for any matter involving disputed facts. The Commission must also provide the authorization holder with all evidence supporting the proposed revocation at the time notice is served, rather than withholding findings or relying on unsubstantiated assertions. CCIA further urges the Commission to preserve formal hearing and appeal rights for any contested revocation matter.

In addition to addressing the concerns over procedural due process guardrails and the proposed response window, CCIA recommends that the Commission strictly limit any revocation proceeding to equipment that, supported by actual evidence of risk, poses a concrete and demonstrable national security threat. Revocations should not be triggered retroactively or mechanically against previously compliant equipment merely because of a subsequent modification to the Covered List. Although the Commission has existing authority to revoke equipment authorizations under 47 C.F.R. § 2.939, that authority is accompanied by procedural protections and should not be converted into automatic revocation whenever the Covered List changes.[61]

X. CCIA strongly supports the Commission's proposal to make software/firmware permissive changes permanent, as these changes would promote efficient product development without implicating national security.[62]

CCIA supports codifying and making permanent the Commission's waiver for already-authorized covered equipment. This is critical to ensure that legacy, lawfully authorized devices

[61] *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").
[62] Third R&O and FNPRM at ¶ 187.

can continue to receive minor updates without losing their authorization status. CCIA also strongly supports a highly flexible equipment authorization framework that accommodates minor, non-security hardware modifications without triggering slow, complex re-authorization processes. Minor hardware component swaps—especially those involving passive, non-security parts—should be handled through streamlined permissive changes rather than formal filings. As drafted, however, proposed § 2.932(b)(4) limits the codification to producer/provider-based entries, excluding location-based sectors like routers, UAS, inverters, and robotics where the waiver is used, while proposed § 2.1043(m) contains no such limit. Extending it to those sectors is worth approximately $22 million a year, before the security value of patches shipping in days rather than the four to twelve weeks a new certification takes.

CCIA is concerned that the condition that acceptable software changes must not "enhance the device's capability"[63] is ambiguous, as all updates are, to some extent, designed to enhance capability by addressing identified flaws (e.g., in managing battery life, protection against unauthorized access, etc.). Ultimately, subjecting routine software modifications to regulatory restrictions or approval gates would undermine security and delay product improvements.

XI. CCIA cautions the Commission that its proposed narrowing of existing pre-authorization operating rules under § 2.805 would severely hamstring American innovation without providing a corresponding national security benefit.[64]

Pre-authorization operation and prototype exceptions serve a fundamentally different purpose than the Covered List. Operating exceptions enable product development, experimentation, and internal evaluation; in contrast, the Covered List is designed to prevent the commercial market entry of insecure finished equipment. Because these units are operated in controlled testing environments and are not being distributed into commercial channels or consumer hands, narrowing or outright removing these exceptions would not provide any benefit to national security. Moreover, narrowing or eliminating operating exceptions would undermine development for any program yet to obtain authorization, creating a severe regulatory gap in

[63] *Id.* at ¶ 193.
[64] *Id.* at ¶ 196.

which lawful operation and evaluation-kit distribution will become legally impossible pending a formal conditional approval.

CCIA recommends that the Commission retain operation and marketing prototype exceptions for all equipment in covered sectors. Standard exceptions (pre-authorization developmental testing and trade show demonstrations) remain highly warranted and essential, even for equipment in covered sectors. Eliminating these exceptions would stifle American innovation and undermine supply chain security.

XII. UAS and Router Covered List Definitions - "Produced in a Foreign Country," "UAS Critical Components," "Routers"[65]

A. CCIA urges the Commission to narrowly interpret "produced in a foreign country," which should be independent of other definitions, and strongly rejects broad, geographic-based dragnets.[66]

In addition to a narrow interpretation of "produced in a foreign country," CCIA urges the Commission against conflating "produced by" (which identifies specifically responsible corporate entities) with "produced in a foreign country" (which defines the geographic scope of production-location-based designations). Merging the two concepts under an expansive standard would create a regulatory dragnet far broader than either test standing alone. Instead, the Commission should focus the definition of "produced in a foreign country" on the location of substantial, device-specific production activity and material decision-making control. We also caution the Commission that including design activities in the definition of "produced in a foreign country" would severely disrupt U.S. manufacturers engaged in cross-border R&D.

CCIA strongly opposes adopting or relying on existing trade or procurement origin tests to define "produced in a foreign country." Specifically, failing to meet the Federal Trade Commission's (FTC) "Made in the USA" standard or the Buy American Act's "domestic end

---

[65] *Id.* at ¶¶ 197-207.

[66] *See id*. at ¶ 198 ("tentatively conclud[ing] that the Commission interpret "produced in a foreign country" to include any equipment that does not qualify as a "domestic end product" as defined in 48 CFR 25.101(a)(1)").

product" cost threshold should not be leveraged by the FCC, as these regimes serve entirely different statutory objectives and are not calibrated to national security threats.

The inverter and robotics determinations adopt the domestic end product test, which the CCIA Research Center estimates requires relocating 37 to 98 percent of a device's value, the upper end reflecting the 75 percent content threshold from 2029.[67] Even Wood Mackenzie's extremely optimistic view of over 100 GW of announced U.S. inverter capacity "by the end of 2027" arrives at the January 1, 2028 Conditional Approval deadline.[68]

Regarding the Commission's interpretation of UAS critical components, CCIA urges the Commission to keep the scope of potential regulation over UAS components strictly bounded. As discussed in this response, any component-level prohibition must focus exclusively on components that actually can be manipulated by adversaries and are relevant to security.

B. CCIA urges the Commission to keep the technical definition of "routers" on the Covered List narrowly tailored to prevent severe industry disruption.[69]

We oppose leveraging domestic end-product component cost percentages to define "routers," as this threshold is completely impractical and would have disastrous implications for the router industry. This definition must remain strictly confined to consumer-grade residential devices and must not bleed into enterprise networking. Revising or expanding this definition in a way that could sweep in enterprise, data center, or infrastructure networking equipment would undermine the very infrastructure necessary to meet the requirements of an ever-evolving economy in which AI plays a crucial role. Any definition should also account for the clarifications that have been incorporated in the FCC's "FAQs on Recent Updates to FCC

[67] CCIA Research Center Study, supra note 2.

[68] Wood Mackenzie, *US Manufacturing Poised to Meet New Inverter Demand Following FCC Ban on Foreign Power Inverters* (Aug. 6, 2026) (reporting announced plans for more than 100 GWac of U.S. PV/PCS inverter manufacturing capacity by the end of 2027).

[69] *See* Third R&O and FNPRM at ¶ 204 ("seek[ing] comment on codifying a definition of "routers" for purposes of the Covered List").

Covered List Regarding Routers Produced in Foreign Countries"[70] and be refined so as not to include devices that have incidental routing functionality or only provide routing in a home (e.g., thread border routers on purely in-home networks).

Consumer grade routers are about $4.2 billion of the $30.8 billion switching and routing customs line (about 14 percent). Approximately six-sevenths of that customs line is the broader universe including enterprise, data-center, and infrastructure equipment a broadened definition would sweep in.[71]

XIII. CCIA strongly opposes the Commission's proposal to impose arbitrary term limits, such as a tentative 10-year expiration date, on equipment authorizations.[72]

For equipment whose relevant design and RF characteristics have not materially changed, imposing an expiration date based solely on the age of the authorization would create massive administrative burdens, disrupt consumers, and threaten infrastructure stability without providing any incremental security benefits. Additionally, the Commission already possesses revocation authority under § 2.939 to address equipment subsequently found to pose a national security threat. Such authority makes rolling expirations redundant and unnecessary.

If the Commission adopts these limits notwithstanding these concerns, they should be prospective only. Before doing so, however, the Commission should 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. The Commission should also give a clear indication of the costs of renewal and the type of supporting paperwork that would need to be in place. 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. Only

[70] Fed. Commc'ns Comm'n, *FAQs: Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries*, FCC, https://www.fcc.gov/faqs-recent-updates-fcc-covered-list-regarding-routers-produced-foreign-countries (May 12, 2026).
[71] CCIA Research Center Study, supra note 2.
[72] Third R&O and FNPRM at ¶ 208.

with these details could CCIA and its members truly assess the potential level of burden that would result from adoption of this type of requirement.

Applied prospectively, a ten-year term would generate no renewal obligation before about 2038. By contrast, applied to the roughly 233,000 authorizations estimated to still be in commercial life, it would cost approximately $47 million per year.[73]

XIV. Registration of SDoC Devices[74]

A. CCIA opposes the Commission's proposal to require that SDoC-authorized devices obtain and display unique, publicly listed ID numbers, which would be highly burdensome for the broader electronics industry.[75]

Requiring registration for SDoC devices would transform a highly efficient self-declaration framework into a de facto premarket approval regime, upending the economic benefits to industry introduced in the first Trump administration and making FCC regulations more draconian than those of its global regulatory counterparts.[76] If the Commission does proceed with establishing such a database, however, the scope of required information should be strictly limited to high-risk devices. CCIA further opposes including HBOM or SBOM data in the scope of required information. Inclusion of this data would be extraneous and burdensome, risk exposing trade secrets, and create massive regulatory bottlenecks. The recurring cost is approximately $18 million per year if limited to high-risk devices, but up to $480 million per year if applied across the Part 15 Subpart B population.[77]

[73] CCIA Research Center Study, supra note 2.
[74] Third R&O and FNPRM at ¶¶ 211-215.
[75] *Id.* at ¶ 213.
[76] *See 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, 8750 ¶ 6 & n.23 (2017) (noting that the Commission did not propose to require RF devices subject to SDoC to be registered in a database); Directive 2014/53/EU, art. 17 & annex II, 2014 O.J. (L 153) 62; Radio Equipment Regulations 2017, SI 2017/1206, regs. 9–11, 41 & sched. 2 (UK).
[77] CCIA Research Center Study, supra note 2.

B. CCIA strongly opposes the Commission's proposal to require online marketplaces to collect and verify SDoC compliance information.[78]

SDoC verification would be an enormous undertaking for online marketplaces, as the universe of SDoC products far exceeds that of certified devices bearing FCC IDs. Aside from these compliance burdens, as well as the burdens associated with proposals previously discussed in this response, this potential rule fails to define the marketplace's legal liability for the accuracy of a third-party seller's statement. As such, unacceptable ambiguity would be created over whether marketplaces would become responsible for determining which product categories require which level of authorization.

C. CCIA recommends that the Commission modernize its portal to provide machine-readable and cryptographic alternatives to manual ID display checks.

Rather than requiring marketplaces to verify FCC IDs, we recommend that the Commission modernize its portal to provide cryptographically signed certifications for programmatic verification, which would allow platforms to confirm legality automatically without manual data scraping. This alternative would be far more efficient for marketplaces than the Commission's proposed mandate for marketplace verification of FCC IDs.

XV. CCIA supports EAS database modernization, as current database limitations make compliance with other proposals (e.g., online marketplace verification and HBOM updates) logistically impossible.[79]

While we support robust communications supply chain security, CCIA is concerned that the Commission's current EAS database is entirely unequipped to support modern compliance and enforcement at scale. Furthermore, prior to potentially requiring submission of a host of additionally sensitive materials, such as HBOMs or SBOMs, upgrades to the EAS to ensure resilience against cybersecurity threats are essential.

---

[78] Third R&O and FNPRM at ¶ 215.

[79] *See id.* at ¶ 216 (seeking comment on suggestions to modernize the EAS database).

Accordingly, no new marketplace verification, accuracy, or display obligations should become effective before the Commission has deployed and tested structured, machine-readable database infrastructure capable of supporting compliance at scale. Imposing such obligations before that infrastructure is operational would create substantial compliance uncertainty and unnecessary administrative bottlenecks. Similarly, any mandates to supply the type of trade secret, competitively sensitive, or otherwise proprietary information contained in HBOMs or SBOMs should not take effect until filers can have sufficient assurance that their submissions are secure.

To address these potential problems, CCIA recommends that the Commission undertake a database modernization effort focused on programmatic data-sharing, structured data fields, and cryptographic information. The Commission also should ensure that its website is adequately secure against cyber-intrusions. Given the Commission's emphasis on the national security importance of equipment authorization activities in the NPRM, and the ongoing nature of proposed filing requirements, the EAS should continue to be available and operational in full during any future government shutdowns. Adoption of these suggestions will reduce the administrative burden on Telecommunication Certification Bodies (TCBs), manufacturers, and marketplaces, and decrease risks to national security.

XVI. If the Commission clarifies or amends how Covered List prohibitions attach to equipment authorizations, CCIA urges establishing strict substantive boundaries.[80]

Component-level authorization bans must be strictly confined to programmable, firmware-bearing, or RF-active components that present plausible cyberattack vectors. Such prohibitions must also completely exclude passive hardware (i.e., capacitors, resistors, and mechanical parts). Covered List bans should apply strictly to direct relationships with designated Covered List entities and not expand into an open-ended inquiry into general foreign manufacturing. Finally, non-covered producers operating within covered sectors (e.g., consumer

[80] *See id.* at ¶¶ 223-224 (seeking comment on "amend[ing] § 2.903(c) to clarify that the prohibitions in paragraphs (a) and (b) apply to all equipment").

routers or robotics) should remain eligible for SDoC authorization rather than being subjected to sector-wide certification bans.

XVII. CCIA warns that the Commission's proposed component-level prohibitions would impose an undue burden on service providers across diverse global supply chains.[81]

Expanding component-level prohibitions beyond logic-bearing hardware would be practically unworkable, impose extraordinary compliance costs, and severely disrupt the deployment of critical computing infrastructure. Enterprise IT hardware and data center equipment (e.g., servers, networking switches, and storage systems) contain thousands of individual components sourced from hundreds of suppliers across multi-tier global supply chains. As previously discussed herein, the R&O drew the correct line by limiting restrictions to logic-bearing hardware, and extending prohibitions to passive or non-RF components would impose crushing compliance overhead without any security benefit.

Furthermore, with the United States at a critical inflection point in building out domestic computing capacity to maintain technological leadership in the face of mounting global competition, the proposed component-level restrictions would slow the speed and scale at which cloud, AI, and enterprise infrastructure is deployed domestically. Converting routine hardware authorization into an exhaustive component-tracing and registration regime would inject massive administrative friction into infrastructure builds, slowing down server deployments across enterprise, commercial, and government cloud environments.

[81] *See id.* at ¶ 226 (seeking comment on "whether and how the determinations made in the [R&O], and the proposals contained in the FNPRM, may affect other existing or proposed certifications, filings, or attestations that reference the Covered List or otherwise require service providers, applicants, or licensees to certify compliance with our equipment authorization or supply chain security rules").

XVIII. While CCIA does not oppose measures reasonably designed to ensure that the Commission can obtain service of process and pursue enforcement against responsible parties, the Commission should not accomplish that objective by requiring foreign manufacturers or distributors to establish a juridical presence in the United States as a condition of accessing the U.S. market.[82]

Trade obligations in both WTO and FTAs (see, for example, Article 15.6 of the USMCA Agreement[83]) prohibit mandating a juridical presence in the United States as a condition for engaging in cross-border sales. Requiring a POC (e.g., law firm) to function as a conduit for service of process would be consistent with trade obligations and should be specifically recognized in the rules. To the extent that stronger safeguards against false information are justified, the FCC should consider requiring the U.S.-based agent to post a bond to address such possibilities, as an alternative to forced establishment. Such an alternative would remain consistent with U.S. trade obligations.

XIX. CCIA urges the Commission to leave realistic, extended transition periods—12 to 24 months minimum—across all sections of this NPRM, especially for HBOM/SBOM requirements and online marketplace verification.

Before any of the FCC's proposals in the NPRM take effect, the Commission must provide clear, multi-stage transition periods, allow for prospective-only application (grandfathering), and meet prerequisite infrastructure milestones, as complex global supply chains, multi-tiered engineering cycles, and e-commerce listing systems cannot adapt overnight.

The Commission's own actions set the benchmark. The R&O itself allows six and nine months for the FCC ID display rules,[84] Conditional Approvals run seventeen to eighteen months, and OET's permissive-change waivers now extend to January 1, 2029. A new certification takes

[82] *See id*. at ¶ 229 (proposing to require a U.S.-based liable party for FCC-certified equipment "to strengthen enforcement of our rules and promote regulatory harmonization by aligning our equipment certification requirements with SDoC requirements").
[83] Agreement Between the United States of America, the United Mexican States, and Canada, Can.-Mex.-U.S., Nov. 30, 2018, T.I.A.S. No. 20-0701.
[84] Third R&O and FNPRM at ¶245.

at least four to twelve weeks per device under current laboratory availability conditions; the HBOM/SBOM, producer-list, and SDoC-registration proposals would impose new collections of information subject to the Paperwork Reduction Act and OMB review, including the Act's applicable public-notice and review requirements.[85] By comparison, the European Union's Cyber Resilience Act ("CRA"), which provides a useful comparator for certain software-supply-chain obligations, entered into force on December 10, 2024, with vulnerability-reporting obligations applying beginning September 11, 2026, and the Regulation generally applying beginning December 11, 2027—providing approximately 21 and 36 months, respectively, for implementation.[86]

XX. Comments on the Initial Regulatory Flexibility Analysis (Appendix D)

CCIA submits the following as responses to the IRFA under the separate heading the Commission requested. The IRFA does not quantify the per-entity burden of any proposal on small entities, although the record permits it. The Commission's own cited source reports that 77 percent of marketplace sellers list fewer than ten products,[87] and the 426,420 sellers it counts (footnote 248) are overwhelmingly small businesses[88] to whom the verification and listing obligations, and any SDoC registration and warning requirements, would attach. On the applicant side, the Equipment Authorization System shows 26,545 original grants in 2025 across 10,440 distinct applicants (about 2.5 grants each)[89] so the HBOM/SBOM requirement (approximately $151 million a year), sector-wide certification (approximately $400 million a

[85] *See* 44 U.S.C. §§ 3506(c)(2), 3507(a)–(b), (d). The PRA generally contemplates a 60-day agency public-comment process for proposed information collections and requires OMB to provide at least 30 days for public comment before acting on a submitted collection.

[86] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements, recital 126, art. 71, 2024 O.J. (L 2847) (Cyber Resilience Act).

[87] Jungle Scout, *State of the Amazon Seller 2025* (Feb. 2025), https://www.junglescout.com/resources/reports/amazon-seller-report-2025/

[88] Amazon, *2025 Small Business Empowerment Report* (Apr. 2026), https://cdn-sellingpartners.aboutamazon.com/7c/18/edd05b224e6b8884a2c7c912d02e/final-sber-report-2025-1.pdf

[89] FCC Office of Engineering and Technology, Equipment Authorization System, original grants issued Jan. 1 to Dec. 31, 2025, by grantee code, retrieved September 1, 2026, https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

year), the thirty-day update rule and the 40-unit importation cap fall largely on small and mid-sized applicants that cannot spread fixed compliance costs across large product lines.[90]

The IRFA also does not evaluate the significant alternatives that would minimize small-entity burden while achieving the Commission's objectives, each of which is set out above: a knowledge or reasonable-diligence standard for producer disclosure; limiting HBOM/SBOM and certification requirements to Covered List sectors and to security-relevant components; a foreign-adversary standard under 15 C.F.R. § 791.4 (formerly § 7.4); prospective-only term limits; a safe harbor for marketplaces keyed to documented process; and extended transition periods.

Section 603(c) of the Regulatory Flexibility Act requires an IRFA to describe significant alternatives that would accomplish the applicable statutory objectives while minimizing significant economic impacts on small entities. In its final regulatory flexibility analysis, the Commission must also explain its selection among significant alternatives affecting small entities.[91]

Conclusion

CCIA supports the Commission's 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 narrow the proposed requirements to address identifiable security risks, preserve workable equipment authorization and R&D pathways, provide appropriate procedural and confidentiality safeguards, and ensure that any new compliance obligations are supported by adequate infrastructure and reasonable

[90] Nicole V. Crain and W. Mark Crain, *The Cost of Federal Regulation to the U.S. Economy, Manufacturing and Small Business* (NAM, Oct. 2023), https://nam.org/wp-content/uploads/2023/11/NAM-3731-Crains-Study-R3-V2-FIN.pdf; *See also* CCIA Research Center Study, supra note 2.
[91] *See* 5 U.S.C. §§ 603(c), 604(a)(6).

implementation periods. CCIA respectfully requests that the Commission take these considerations into account as it develops any final rules in this proceeding.

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 8, 2026