Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to	)	ET Doc. No. 21-232
The Communications Supply Chain through the	)	
Equipment Authorization Program	)	

Comments of the Telecommunications Industry Association

Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard, Floor 9
Arlington, VA 22209

September 8, 2026

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to	)	ET Doc. No. 21-232
The Communications Supply Chain through the	)	
Equipment Authorization Program	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. Introduction and Summary

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide input regarding the Third Further Notice of Proposed Rulemaking ("FNPRM") issued by the Federal Communications Commission ("Commission" or "FCC") in the above-captioned proceeding.[1] TIA is a U.S.-based trade association representing more than 400 trusted global manufacturers and vendors of telecommunications equipment. TIA members design, manufacture, and manage the world's digital infrastructure and information communications technology ("ICT") devices. TIA is also a standards-developing organization with a more than 80-year history of developing thousands of technical standards that allow ICT equipment and networks to operate efficiently and effectively.

In this role, TIA has long supported the FCC's work to protect U.S. networks from threats posed by foreign adversaries, including through effective implementation of the Secure

[1] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Third Report & Order, Third Further Notice of Proposed Rulemaking, ET Doc. No. 21-232 (Jul. 22, 2026) ("Report and Order" or "FNPRM").

Networks Act and Secure Equipment Act.[2] As our world becomes increasingly interconnected and reliant on connectivity, trusted manufacturers share the U.S. government's interest in ensuring foreign adversaries cannot exploit control over suppliers to exfiltrate sensitive data, disrupt critical functions, or otherwise compromise the security of U.S. networks.

Protecting this interest requires both targeted and coordinated action to address suppliers that pose such threats, as well as collaborative policy efforts to build a regulatory environment that fosters a robust trusted international supply base. With more than 80% of American critical infrastructure owned and operated by the private sector, companies must be empowered partners that can optimize resources for operational collaboration on network defense and forward-looking risk management. With rapid growth in AI, data centers, advanced computing applications, and unprecedented demand for key components, amid a shifting geopolitical landscape, regulatory predictability will also pay national security dividends as manufacturers navigate dynamic and evolving supply chain challenges.

With these goals in mind, TIA urges the Commission to act on the proposals of the FNPRM in line with the following five guiding principles:

1. *Grounded in Specific National Security Determinations*: Covered List restrictions should remain tied to the specific nature and scope of the underlying national security determination,
2. *Bifurcation:* Producer/provider-based and production location-based determinations are inherently different and should be treated as such,
3. *Narrowly Tailored to Security:* New compliance obligations and administrative burdens should be narrowly tailored to the specific national-security concern they

[2] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) ("Secure Networks Act"); Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 (Statutory Notes and Related Subsidiaries)) ("Secure Equipment Act"). See, e.g., Comments of TIA, ET Docket No. 21-232 & 21-233 (Sept. 20, 2021); Reply Comments of TIA, ET Docket No. 21-232 & 21-233 (Oct. 18, 2021); Comments of TIA, ET Docket Nos. 21-232 & 21-233, (Apr. 7, 2023); Reply Comments of TIA, ET Docket No. 21-232 & 21-233 (May 8, 2023); Comments of TIA, ET Doc. No. 21-232 (Jan. 5, 2025); Reply Comments of TIA, ET Doc. No. 21-232 (Feb. 2, 2026).

seek to mitigate and should not impose unnecessary burdens on trusted manufacturers who pose no clear national security risk,

4. *Preserve Existing Flexibility:* In addressing newfound security concerns, the Commission should refrain from enacting proposals that would restrict existing flexibility within the equipment authorization process that is necessary for innovation, product development, and supply-chain resiliency,
5. *Targeted Action:* The Commission should prioritize targeted enforcement against bad actors and modernization of existing Commission databases and compliance tools rather than impose broad, overburdensome marketplace-wide obligations.

To that end, we caution the FCC against proposals in the FNPRM that would not deliver material national security improvements – including many of the proposed disclosure, reporting, and reauthorization requirements. In practice, such proposals would significantly impede the equipment authorization process, stymie innovation and availability for consumers, raise costs for industry and consumers alike, and ultimately undermine U.S. technology leadership and competitiveness. The existing equipment authorization process was designed to evaluate device compliance with the Commission's technical rules, not to serve as a comprehensive supply-chain reporting regime, a process which should be left to industry-led standards and best practices.

Instead, the Commission can achieve its goal of ensuring effective implementation of Covered List restrictions by: (i) clearly articulating the extent of the Covered List restrictions (e.g., regarding covered components and the "produced by" definition) with distinctions between "producer/provider-based" and "production location-based" categories; (ii) codifying recent permissive change waivers regarding software and hardware to provide smooth and secure transition periods following Covered List updates; (iii) updating attestation requirements to reflect these new rules and working with stakeholders to educate, investigate, and enforce; (iv) providing sufficient transition periods for any new requirements sufficient for industry to comply and the Commission to create the necessary tools for compliance; and (v) modernizing existing

compliance tools and databases to improve enforcement and transparency without imposing new reporting obligations.

II. The Commission Should Implement the Covered List Prohibitions in a Manner that is Tailored to the National Security Determination Underlying Each Listing

a. Covered List Restrictions Remain Bound by the Scope Intended by the Secure Networks Act

In the Secure Networks Act, Congress made the Commission the caretaker of a new, discrete tool aimed at preventing foreign adversaries from exploiting untrusted equipment embedded in U.S. networks. In placing the Covered List under the Commission's charge, the Secure Networks Act itself directed the Commission to update the Covered List based *solely* on specific determinations made by enumerated sources, rather than granting the Commission authority to make these national security determinations on its own.[3] This approach was designed to ensure that the extraordinary act of designating companies as national security threats (and then barring their access to the U.S. market) is done only where national security experts leverage their unique expertise and intel to inform a risk-based decision about the scope, timing, and target of such a prohibition. Ideally, it also helps ensure that such an action is coordinated with national security efforts across other agencies with the potential for overlapping impacts.

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

To that end, when considering the proposals raised in the FNPRM, TIA urges the Commission to view any requirements and policies adopted through this proceeding through the narrowly tailored scope explicitly authorized in the language of the Secure Networks Act.

b. *The Commission Correctly Proposes to Distinguish Producer/Provider-Based and Production Location-Based Covered List Determinations*

TIA strongly supports the Commission's recognition that the "producer/provider-based" and "production location-based" categories of the Covered List must be treated distinctly. In proposing to bifurcate its Covered List rules, the Commission recognizes that these categories reflect fundamentally different national security risks and challenges in implementation and therefore warrant distinct regulatory treatment.

Restrictions directed at specific entities that pose a demonstrable risk to national security are materially different from restrictions that apply to an entire category of products based on their location of production. Producer/provider-based Covered List determinations generally reflect a finding regarding the trustworthiness of a particular entity, often one that has been determined by the named, relevant national security agency to be subject to the ownership, control, or influence of a foreign adversary. Production location-based determinations, by contrast, are broader in scope and generally reflect concerns regarding supply chain exposure associated with where equipment is manufactured rather than the conduct or trustworthiness of a specific company. As a result, the risks presented by these two categories are different, and the Commission's implementation of the Covered List should reflect those differences.[4]

[4] FNPRM at ¶ 129

This distinction is particularly important because many of the Commission's existing Covered List rules were developed during a period in which all Covered List designations were producer/provider-based, as initially envisioned by the Secure Networks Act.[5] From the establishment of the Covered List in 2018 until the end of last year, every expansion of the Covered List as well as past restrictions on the Commission's equipment authorization process, reporting obligations, and related compliance requirements reflected concerns associated with specifically identified entities. As the Commission itself recognizes in both the Third Report and Order and this FNPRM, certain restrictions that may be appropriate when applied to a specific producer or provider are not appropriate when applied to entire categories of equipment based solely on production location. In the Third Report and Order, for instance the Commission determined to only apply new "logic bearing hardware component" prohibitions to producer/provider-based categories.[6] Likewise, the FNPRM appropriately seeks comment on whether a variety of existing reporting, disclosure, and compliance requirements should continue to apply in the same manner to production location-based Covered List equipment. These questions are well-founded because many requirements built around the Covered List were designed to address concerns associated with specific entities, not broad classes of products that may encompass substantial portions of a global supply chain.

The practical consequences of production location-based Covered List determinations further underscore the need for tailored regulatory treatment. By their nature, production location-based restrictions are substantially broader than producer/provider-based restrictions

[5] See eg. *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Report & Order, Order, and Further Notice of Proposed Rulemaking, ET Doc. No. 21-232 (Nov. 25, 2022) (initial designation of Huawei and ZTE).
[6] Report and Order at ¶¶ 14-36.

and can immediately affect entire categories of devices. Such determinations can temporarily constrain access to broad segments of the marketplace while manufacturers pursue potential Conditional Approvals from the Administration, diversify manufacturing operations, or transition production capacity as applicable. Accordingly, requirements that may be workable when applied to a discrete set of identified named and known entities can become significantly more burdensome, and in some cases unworkable, when applied across an entire product category.

For these reasons, TIA agrees with the Commission that identical regulatory treatment of these distinct determinations is neither necessary nor appropriate. Rather, the Commission should continue evaluating Covered List requirements through the lens of the underlying national security determination that gave rise to the listing. While many of the Commission's most burdensome restrictions might be necessary for specific, identified national security risks associated with a specific entity, they should generally be limited to producer/provider-based Covered List categories due to the lower risk and higher implementation burdens involved in such producer/provider-based determinations.

Accordingly, TIA supports the Commission's proposal to clarify that certain existing rules apply only to producer/provider-based Covered List categories and encourages the Commission to continue assessing whether additional requirements should likewise be limited to those categories. Maintaining this distinction will help ensure that Covered List implementation remains appropriately tailored to the national security concerns at issue while avoiding unnecessary harms to the global ICT marketplace, creating burdensome requirements for trusted manufacturers that do not pose a significant national security risk, and significantly disrupting the equipment authorization process on which the global ICT marketplace depends. Likewise,

TIA urges the Administration to continue refining production-location based determinations to ensure that they are closely tailored to mitigate the underlying national security threats that necessitate the determination.

c. The Commission Should Clarify the Meaning of "Produced By" While Preserving Beneficial White-Labeling Practices

TIA appreciates the Commission's efforts to clarify what activities should be considered "production" for the purposes of the Covered List. TIA also understands the Commission's interest in preventing entities identified on the Covered List from circumventing those restrictions through white-labeling arrangements or similar practices. The Commission can advance both objectives by adopting clear and administrable definitions that target genuinely problematic conduct without disrupting legitimate and longstanding business practices that benefit product diversity throughout the ICT ecosystem.

To that end, we support the Commission's proposed definition of "produced by," whereby a device is "produced by" an entity "if that entity exercises substantial responsibility for, or control over, any major stage of the process by which the device comes into existence, including the design, manufacturing, assembly, or development of the device. A device may be 'produced by' more than one entity."[7] This definition appropriately focuses on meaningful participation in the creation of a device, rather than relying solely on ownership, formalistic branding-based distinctions, or distribution arrangements.

Further, the definition should encompass licensed intellectual property from producer/provider-based Covered List entities where the identified producer or provider retains

[7] FNPRM at ¶ 134.

substantial responsibility for, or control over, a major stage of production. However, the Commission should make clear that ordinary commercial relationships, including participation in standards-development activities and contributions to internationally recognized technical standards, do not by themselves constitute "production" for purposes of the Covered List restrictions.

For example, many trusted suppliers rely on specialized third parties to provide discrete services or licenses related to product design, engineering, manufacturing, development, or marketing while continuing to sell products under their own brand. These arrangements reflect longstanding commercial practices that enable companies to leverage specialized expertise, increase efficiency, expand consumer choice, and foster competition. The Commission should clarify that these types of commercial relationships are not inadvertently swept within the scope of the "produced by" definition, as doing so could create uncertainty for legitimate supply-chain and product-development practices that benefit consumers and promote innovation without introducing national security risks. Such clarification would additionally help provide regulatory certainty while ensuring the rules remain focused on the national-security concerns that gave rise to the Covered List designation. By contrast, the Commission should avoid imposing additional requirements that would effectively discourage beneficial white-labeling practices. White-labeling arrangements are a common feature of the global ICT marketplace, allowing companies to specialize in component development, engineering, manufacturing, branding, and marketing. These arrangements promote innovation, competition, and consumer choice, while enabling firms to leverage comparative advantages across different segments of the value chain.

d. The Commission Should Continue Tailoring Covered List Prohibitions Based on the Underlying National Security Determination

As the Commission considers additional requirements for Covered List entities, it should continue to weigh whether restrictions are appropriately tailored to the national-security determination that gave rise to the listing in the first place. The Commission's proposed bifurcation framework provides a useful foundation for this analysis and should guide implementation decisions throughout this proceeding.

As discussed above, restrictions and limitations on producer/provider-based equipment may be appropriate in certain contexts, but the Commission should refrain from automatically extending all restrictions and burdens to all Covered List determinations, including production location-based determinations. To that end, TIA supports the FNPRM's proposal to narrow submarine cable compliance requirements so that they apply only to producer/provider-based Covered List determinations.[8] This approach appropriately considers the global nature of subsea cable infrastructure and aligns with U.S. security concerns while avoiding unnecessary disruption to the global subsea cable network.

More broadly, the Commission should continue assessing future Covered List requirements through the lens of the specific national-security determination that gave rise to a particular listing and provide industry the necessary flexibility to continue to operate in a global market where possible. Doing so will help ensure that Covered List implementation remains both effective and sustainable, while avoiding the unintended consequences that can arise when requirements developed for one type of national-security concern are applied indiscriminately to another.

[8] FNPRM at ¶¶ 217-222

e. *The Commission Should Not Extend Covered List Prohibitions to All Components and Firmware/Software from Covered List Entities*

TIA supports the critical, narrowly tailored role the Commission must play to ensure that U.S. networks are built from trusted components. However, the Commission should not, at this time, extend Covered List prohibitions to all components of a Covered List entity merely because a supply chain dependency exists. As discussed above, the Secure Networks Act is clear on the specific role the FCC must play when adding an entity to the Covered List, and the Commission does not independently possess the authority to determine that general supply chain dependencies involving Covered List entities create a national security risk.[9] At this time, no such specific determination has been made with respect to all components produced by Covered List entities.

This distinction is important because many components do not present the type of risks contemplated by the statute or reflected in existing specific determinations by enumerated sources that trigger a Covered List addition. In particular, numerous components, including many non-logic-enabled hardware components, lack the advanced functionality and security risk that has traditionally formed the basis for Covered List-related concerns. Extending Covered List prohibitions to all components, regardless of their capabilities or role within a device, would therefore extend considerably beyond any existing specific determinations reflected in the Covered List and could create substantial disruption throughout global supply chains.

For similar reasons, the Commission should proceed cautiously before extending Covered List restrictions further into the software and firmware context. There are existing

[9] In addition, neither the passing references to "national security" in the Communications Act or authority to regulate devices to prevent harmful interference empower the Commission to adopt the proposals to address supply chain dependencies via the proposed all-components ban.

specific determinations made by enumerated sources that have found that certain software products pose unacceptable national-security risks.[10] The inclusion of software products such as those associated with Kaspersky Labs on the Covered List demonstrates that the existing framework is capable of addressing software-related concerns where the appropriate national security determination has been made, although no such determination has been made that generally applies to software or firmware of any and all Covered List entities, in perpetuity.

Any broader software-related framework must continue to recognize the important distinction between producer/provider-based and production location-based Covered List categories. Software presents a unique set of implementation challenges, including questions regarding provenance, updates, third-party dependencies, and the use of open-source code. These challenges counsel in favor of a measured approach that remains closely tied to the specific national-security determinations underlying the Covered List rather than broad prohibitions that may prove difficult to administer or enforce in practice.

III. The Covered List Does Not Justify Significantly Transforming the Equipment Authorization Program by Requiring Broad Supply Chain Disclosures

TIA appreciates the Commission's efforts to add transparency and increase the resiliency of ICT supply chains. Ensuring that the ICT supply chain is composed of equipment from trusted vendors and manufacturers has been a longstanding focus of TIA as the industry association for trusted manufactures around the world. The goal of adding transparency to supply chains and reducing exposure to untrusted vendors and manufacturers is why TIA created our supply chain security standard, SCS 9001. We have been working with the U.S. government

[10] *See, e.g. Final Determination: Case No. ICTS-2021-002, Kaspersky Inc.,* Department of Commerce, Bureau of Industry and Security, 89 Fed. Reg. 52,956 (June 24, 2024).

to advocate for trusted vendors in countries around the world, and we believe the way to build trusted networks is through the adoption of industry-led standards such as SCS 9001. By contrast, broad government mandates, which treat all manufacturer's supply chains the same risk imposing unnecessary burdens on trusted manufacturers' that are not tailored to mitigate an existing security threat. This in turn may prevent such trusted manufacturers from participating in the U.S. market and raise costs on these vendors both domestically and abroad as they strive to compete with entities sponsored by foreign adversaries. To that end, we urge the Commission to support industry-led standards aimed at increasing transparency and mitigating risk in supply chains, as opposed to adopting reforms that would significantly transform and disrupt the Commission's existing equipment authorization process.

a. *The Commission Should Not Adopt Broad HBOM and SBOM Requirements*

As the Commission is aware, supply chain transparency can serve an important role in identifying and addressing national security risks in certain circumstances. However, adopting broad hardware bill of materials ("HBOM") or software bill of materials ("SBOM") disclosure requirements in the equipment authorization process at this time would be costly – if not potentially infeasible – and may actually undermine the Administration's goals. Discussions with TIA members indicate that it is not possible at present to implement such requirements in a consistent, automated, and administrable manner across the ICT equipment ecosystem; these requirements would impose significant burdens on manufacturers, Telecommunication Certification Bodies ("TCBs"), and the Commission itself without delivering commensurate national-security benefits.[11]

[11] *See generally* FNPRM at ¶¶ 139-146.

The Commission's existing equipment authorization framework already contains multiple safeguards designed to ensure compliance with the Covered List and related national security requirements. Equipment authorization applicants must ensure that marketed devices remain identical to tested samples, comply with the Commission's authorization requirements, and satisfy applicable attestation obligations concerning Covered List equipment and entities.[12] These requirements ensure accountability for authorized devices while allowing manufacturers to responsibly manage complex global supply chains. In light of these existing protections, broad HBOM or SBOM disclosure obligations would not materially improve national security outcomes. Further, requiring a provenance filing would also institute a new obligation expanding regulatory requirements on manufacturers at a time when the Commission has been focused on reducing such unnecessary burdens.[13] The equipment authorization process already provides the Commission with detailed technical information about each certified ICT device – including circuit descriptions, block diagrams, schematics, and photographs of internal construction – none of which currently require the submission of a full bill of materials.

Instead, the Commission should continue relying on applicant attestations regarding Covered List equipment and software incorporated into authorized devices. Such attestations provide a practical and enforceable mechanism for ensuring compliance with Covered List prohibitions while avoiding the substantial administrative complexities associated with maintaining and continually updating detailed hardware and software inventories for every authorized product. Indeed, where the Commission's concern is whether a device incorporates Covered List equipment or software, a targeted attestation requirement is both more direct and

[12] *See generally* Supplier's Declaration of Conformity, 47 CFR §§ 2.906; 2.907; 2.911.
[13] *See generally Delete, Delete, Delete*, GN Doc. No. 25-133 (Mar. 12, 2025).

more administrable than requiring the submission of expansive HBOMs and SBOMs that may contain thousands of individual entries but provide little additional insight into the specific national-security concern at issue.

The practical realities of modern ICT manufacturing further demonstrate why broad requirements for continually updated HBOMs and SBOMs are ill-suited for the equipment authorization process. The ICT industry operates on a global scale and manufactures products at tremendous volume. A single device may incorporate components sourced from multiple suppliers and production facilities and may be assembled in different locations depending on demand, availability, and ordinary supply-chain fluctuations. As a result, the hardware composition of a particular device may vary over time or across production runs while remaining fully compliant with the Commission's equipment authorization requirements. Manufacturers rely on this flexibility to respond to supply chain disruptions, source commodity components efficiently, control costs, and continue delivering products to consumers while maintaining oversight and responsibility for the authorized device.

Moreover, supply chains are dynamic throughout any given product's lifecycle. Components may change due to market availability, supplier transitions, manufacturing efficiencies, security updates, or other operational considerations. As a result, HBOM and SBOM submissions would quickly become outdated. Manufacturers would either be required to continuously update those submissions throughout a product's lifecycle or risk potential enforcement exposure based on information that no longer accurately reflects the product as produced and marketed. Such an approach would impose substantial ongoing compliance burdens and overhead costs while providing information that may be stale almost immediately after submission.

Should the Commission adopt any kind of HBOM requirement, to protect good faith applicants and grantees operating complex global supply chains, the Commission must establish safe harbor protections against unauthorized or unapproved component substitutions made by third-party contract manufacturers.[14] Where an applicant or grantee exercises reasonable due diligence – such as incorporating strict contractual prohibitions, auditing supplier components, and conducting HBOM verification – an unapproved part substitution by a contract manufacturer during production or global component shortages should be treated as an isolated vendor breach. Such actions should not be treated as an immediate, willful violation by the applicant or grantee that triggers automatic grant revocation or enforcement penalties against the authorization holder.

The Commission should also recognize that at present there is no universally accepted methodology or format for demonstrating the details of a product's hardware and software supply chains at the level contemplated by the FNPRM.[15] Although industry, government, and standards organizations continue to explore approaches for improving software and supply chain transparency, no globally accepted framework currently exists that would ensure manufacturers provide comparable, machine-readable, and consistently structured HBOMs and SBOMs. As a

[14] The component swap envisioned would be consistent with the device's authorization.

[15] As the Cybersecurity and Infrastructure Security Agency ("CISA"), National Security Agency, Federal Bureau of Investigation, and international partners explained in the recent update of Minimum Elements for an SBOM, "SBOM implementation – how the data is generated, shared, analyzed, and otherwise used – differs widely, in part due to the variety of SBOM use cases." 2026 CISA Minimum Elements for a Software Bill of Materials (CISA et al., *2026 Minimum Elements for a Software Bill of Materials* (SBOM), at 7 (July 29, 2026)), https://www.cisa.gov/sites/default/files/2026-07/2026_cisa_sbom_minimum_elements_508c.pdf. Likewise, CISA's HBOM Framework describes how "current HBOM formats need some assistance to be portable between suppliers and purchasers," stating that "further work will be required to achieve the necessary maturity for true interoperability." CISA, *A Hardware Bill of Materials Framework for Supply Chain Risk Management*, at 2 (Sep. 2023), https://www.cisa.gov/sites/default/files/2023-09/A%20Hardware%20Bill%20of%20Materials%20Framework%20for%20Supply%20Chain%20Risk%20Management%20%28508%29.pdf.

result, the Commission would likely receive submissions that vary significantly in scope, detail, format, and usefulness.

Even leading open standards for supply chain reporting – such as SPDX and CycloneDX – are still maturing and face significant operational hurdles. Current industry tools lack uniform implementation, resulting in field-level ambiguities regarding identifiers and hashes, persistent gaps when tracing proprietary sub-components, and inconsistent outputs across suppliers.[16] In addition to these technical limitations, open standards are designed to identify legal corporate entities, not to map physical factory locations across multi-site semiconductor design, wafer fabrication, assembly, and testing, for example. Attempting to mandate granular geographic tracking or custom reporting beyond established open formats would impose severe compliance burdens on industry without delivering actionable national security value to the Commission.

The challenges presented by software are even more significant. Modern software products frequently incorporate open-source libraries, third-party dependencies, and continuously updated code bases that may evolve throughout the life of a product. This is by design and enables manufacturers to maintain and, often, enhance their products within the bounds of the Commission's equipment authorization framework. Determining what software components must be included in an SBOM, how indirect dependencies should be treated, how open-source contributions should be categorized, and how updates should be reported raises a host of unanswered practical questions. These challenges are particularly acute for

[16] *See generally* Comment of Information Technology Industry Council on CISA-2025-07: 2025 Minimum Elements of a Software Bill of Material (Oct. 3, 2025) (*available at* https://www.regulations.gov/comment/CISA-2025-0007-0054).

communications equipment that relies on complex software stacks maintained by multiple vendors and open-source communities. Absent clear, globally accepted methods and reporting practices, SBOM requirements risk becoming a costly documentation exercise rather than a meaningful security tool.

Fortunately, HBOM and SBOM requirements are not necessary to fulfill the Commission's obligations under the Communications Act. The Secure Networks Act and the Secure Equipment Act, incorporated into the Communications Act, require the Commission to implement specific national security determinations reflected in the Covered List and to ensure that covered equipment is not authorized in contravention of those determinations.[17] The Communications Act does not, however, mandate and authorize the creation of a broad supply chain regulatory regime for authorized communications equipment. Accordingly, the Commission should be cautious before transforming the equipment authorization process into a vehicle for collecting and maintaining detailed supply chain information that extends well beyond the statutory framework established by Congress.

If the Commission nevertheless determines that some form of HBOM or SBOM requirement is necessary, it should significantly narrow the proposal. At most, any such requirements should be limited to equipment associated with producer/provider-based Covered List categories rather than broadly applied across all Covered List sectors. As discussed above, producer/provider-based Covered List determinations reflect specific findings regarding identified entities and therefore have a much closer nexus to the types of transparency concerns the Commission seeks to address in this proceeding than categorical production-location based

[17] Secure Networks Act, Section 2(b).

determinations or all equipment put forward for authorization. Extending HBOM or SBOM obligations beyond that context would dramatically increase compliance burdens while providing little corresponding benefit. To the extent the Commission mandates reporting , it should restrict requirements to established open data standards – such as SPDX or CycloneDX – and focus strictly on legal manufacturer entities. While these open frameworks face ongoing maturity hurdles (as detailed above), anchoring any requirement to their standardized corporate-entity fields is essential to avoid two unworkable outcomes: (1) attempting to track disaggregated, multi-site physical component geography, and (2) creating a custom, non-standardized reporting regime that existing automated tools cannot support.

Further, the Commission must take significant steps to ensure it does not create larger, more significant security risks by requiring production of HBOM or SBOM information than it purports to solve. Counter to the intent of the Secure Networks Act, any public disclosure of an HBOM or SBOM could itself introduce a security risk to U.S. networks by identifying for potential adversaries which devices rely on a given component or highlighting components embedded within U.S. networks that suffer from a known vulnerability. Such information could also be used as a roadmap by bad actors to counterfeit devices. Competitors could also capitalize on these details to gain an economic edge in the global marketplace against U.S. and trusted ICT vendors, compromising American technological and economic leadership abroad. Any bill-of-materials information provided to the Commission should therefore only be furnished upon a specific request concerning an identified device and should be protected as confidential. If the Commission insists on the filing of HBOM and SBOM materials as part of the equipment authorization process, it must provide industry automatic and permanent confidential treatment of these issues and shield them from public disclosure. The Commission must also significantly

invest in upgrading and hardening its existing databases from cyber threats of bad actors, both rogue and state sponsored, if it intends to collect such granular details about U.S. networks and critical infrastructure technology.

Additionally, any adopted framework should include reasonable transition periods, apply only prospectively, incorporate appropriate de minimis thresholds, and avoid requiring disclosures beyond first-level components or material software contributions. Industry would need substantial time to develop the processes, internal controls, supplier arrangements, and reporting systems necessary to generate the type of HBOMs and SBOMs contemplated by the FNPRM. At minimum, the Commission should provide industry four years to implement such a requirement. Even then, significant challenges would remain with respect to standardization, maintenance, ongoing updates, and upgrades to network infrastructure necessary to ensure that the information being sought, which includes some of the most sensitive trade secrets these companies possess, is accorded requisite protections.

Finally, the Commission should preserve manufacturers' abilities to manage routine sourcing decisions within the bounds of the existing equipment authorization framework. Particularly for commodity components, manufacturers must remain free to respond to supply-chain disruptions and market conditions while ensuring that marketed devices remain consistent with authorized designs. The Commission's equipment authorization rules already provide reasonable mechanisms for evaluating changes to authorized equipment. Broad HBOM and SBOM requirements should not become a means of restricting ordinary supply-chain management practices that historically have not raised national security concerns.

The Commission should also decline to adopt the proposed percentage-of-value element.[18] This proposal does not include necessary specifics to be properly vetted by industry and commentors alike, such as which cost measure the Commission would use, when it would be measured, or how such a value would be allocated in circumstances where a singular component is produced in multiple locations. Since it is common for components to be multi-sourced, many manufacturers do not have a static percentage available that could be consistently reported to the Commission, especially under an attestation that carries the potential penalty of forfeiture.

For all these reasons, TIA urges the Commission to decline to adopt any HBOM or SBOM requirements. The Commission can more effectively address Covered List concerns through targeted attestation requirements and focused enforcement mechanisms than through a sweeping disclosure framework that would burden industry, complicate equipment authorization, and produce information that may be difficult to standardize, verify, or meaningfully utilize.

b. *The Commission Should Preserve the Benefits of the Supplier's Declaration of Conformity Framework*

The Commission should also be wary not to undermine the substantial benefits achieved through its modernization of the equipment authorization framework in response to Covered List concerns. In particular, TIA opposes proposals that would effectively eliminate or significantly narrow the Supplier's Declaration of Conformity ("SDoC") process for broad categories of equipment that have historically been eligible for that pathway. As TIA has raised numerous times before the Commission, its 2017 equipment authorization reforms that created the current SDoC framework provides a streamlined and efficient means of demonstrating compliance for a wide range of devices; it has reduced unnecessary administrative burdens on both industry and

[18] FNPRM at ¶ 142.

the Commission.[19] Those reforms have been viewed as a success by industry and have modernized the equipment authorization process, reduced barriers to innovation, and enabled manufacturers to bring compliant products to market more efficiently, to the benefit of U.S. consumers, the economy, and the nation's global leadership, without compromising the Commission's ability to enforce its rules.

As TIA has cautioned in the ongoing proceeding examining authorization of Commission testing facilities, the Commission should be wary of any effort to restrict the use of this successful process without providing information on why such restrictions would mitigate significant national security concerns.[20] In the absence of a demonstrated national security benefit, the Commission therefore should not require certification for all devices falling within Covered List sectors. Such an approach would represent a significant departure from the existing equipment authorization framework and would become increasingly burdensome as the scope of Covered List updates expands over time. Production-location based additions to the Covered List have occurred with no notice to industry, hampering the ability to adjust carefully calibrated procurement and launch timelines to these sudden and immediately effective designations. These additional burdens would come at a time where the global testing industry is already under significant strain through capacity issues caused by the revocation of previously authorized labs and increased demand that comes with any significant next-generation technical advancement. While the results of pending public notices on market surveillance and

[19] *See* Comments of TIA, ET Doc. No. 24-136 (Sept. 3, 2024); Reply Comments of TIA, ET. Doc. No. 24-136 (Oct. 2, 2024); Comments of TIA, ET. Doc. No. 24-136 (Aug. 15, 2025); Comments of TIA, ET Doc. No. 24-136 (Jul. 15, 2026).
[20] Comments of TIA, ET Doc. No. 24-136 (Sept. 3, 2024); Reply Comments of TIA, ET. Doc. No. 24-136 (Oct. 2, 2024).

streamlining of procedures for trusted labs could alleviate some concerns, the testing ecosystem will not be able to adjust until decisions are issued and new procedures are implemented.

Critically, the FNPRM does not demonstrate that eliminating the flexibility afforded by the SDoC process would meaningfully improve national-security outcomes. The relevant question is whether a device incorporates covered equipment or is produced by a covered entity, not whether the device was authorized through certification or SDoC. Specific entities named by the Covered List are already barred from the process, and any further revocation of SDoC benefits from trusted entities that manufacture equipment identified by a Covered List category would insufficiently address a national security concern while potentially leading to negative economic outcomes, keeping new innovations our of the hands of U.S. consumers, and hampering U.S. global ICT leadership.

Similar concerns apply to the Commission's proposal to require registration of SDoC devices and the assignment of unique identifiers. Requiring all SDoC devices to register with the Commission would fundamentally alter the nature of the SDoC framework and erode many of the efficiencies it was designed to deliver. Existing Commission enforcement authorities already provide mechanisms for investigating and addressing non-compliant devices, and the record does not demonstrate that a comprehensive registration requirement is necessary to address Covered List concerns. As is the case with the Commission's HBOM and SBOM proposals, upgrades to the FCC equipment authorization system to manage the sheer capacity of registrations would almost certainly be a prerequisite to implementation of any such requirement.

More broadly, many of the FNPRM's proposed certification, registration, and disclosure requirements share a common flaw: they reduce existing regulatory flexibility and substantially

increase administrative burdens without a demonstrated nexus to improving national security.[21] The Commission should instead build upon the success of its existing equipment authorization modernization efforts, including the efficiencies made possible through the E-LABEL Act and related reforms, rather than layering new procedural requirements onto processes that are already functioning effectively.[22]

Accordingly, TIA urges the Commission to preserve the flexibility inherent in the SDoC framework and focus its efforts on targeted compliance and enforcement measures directed at actual national-security risks, rather than broad procedural requirements that would burden the entire equipment authorization ecosystem.

IV. The FCC Should Codify Additional Permissive Change Waivers For Covered Equipment

TIA supports the Commission's proposal to codify a framework permitting certain Class I and Class II permissive changes to previously authorized covered equipment.[23] The Commission's recent waiver orders appropriately recognized that maintaining the security, reliability, and functionality of communications equipment requires manufacturers to retain limited flexibility to update authorized devices following Covered List designations.[24] Codifying the types of changes permitted in these waivers would provide regulatory certainty for manufacturers while ensuring that consumers and network operators continue to receive critical software, firmware, and hardware updates.

---

[21] *Infra*, Section V (discussing existing compliance burden for FCC labeling requirements).
[22] E-LABEL Act, 47 U.S.C. § 609 note (2018).
[23] FNPRM at ¶¶ 187-195
[24] *See, e.g.*, *NCTA – The Internet & Television Association Petition for Expedited Waiver to Permit Targeted Class I and Class II Permissive Hardware Changes to Covered Routers*, ET Doc. No. 21-232, Order, DA 26-571 (rel. June 9, 2026), *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Order, ET Doc. No. 21-232 (Jun. 9, 2026).

As proposed, the Commission should revise its rules to allow software and firmware updates intended to mitigate harm to U.S. consumers as a matter of course for both producer/provider-based and production location-based Covered List equipment. Security vulnerabilities do not disappear when equipment becomes subject to Covered List restrictions. To the contrary, limiting manufacturers' ability to deploy security updates could inadvertently increase risk by preventing the remediation of known vulnerabilities in existing devices. Allowing such updates promotes the Commission's national-security objectives while protecting consumers and preserving confidence in communications networks. The Commission should likewise permit limited Class I and Class II hardware changes, including minor component replacements. As discussed throughout these comments, the global ICT supply chain is dynamic and requires manufacturers to respond to changing market conditions, component availability, and supply-chain disruptions. Providing a clear pathway for narrowly tailored hardware modifications will help ensure continuity of supply while preserving the integrity of the equipment authorization process.

TIA also urges the Commission to not bar the replacement of a U.S. produced component in an authorized device with a foreign-produced one. It is common practice for manufacturers to make these substitutions due to a component reaching end-of-life phase, or when it is no longer readily available. In such circumstances, the availability of a high-quality substitute is paramount, and adding mandates for country of production for such components could significantly impact supply chain resiliency and create disruptions in device availability. Such requirements could also introduce supply chain risks by increasing single source dependency. Additionally, the Commission should confirm that any qualifying update to an authorized device will not be treated as a new application for equipment authorization, and that a device receiving

such an update still retains its existing grant and identifier. This would allow routine security maintenance to proceed without fear that such updates would trigger any sort of re-authorization requirement.

More broadly, the Commission's approach to permissive changes reflects several of the principles that should guide this proceeding. Rather than imposing new reporting obligations or restrictions, the permissive change framework adopts a targeted, risk-based approach that continues to advance national security objectives while preserving the flexibility necessary for innovation, product maintenance, and supply chain resiliency.

V. The Commission Should Preserve Flexibility Necessary for Industry to Innovate, Develop Cutting Edge Products, and Address Emerging Supply Chain Risks

a. Limiting Access to ODM, OEMs, and Similar Third-Party Vendors Will Increase Costs Without Enhancing National Security

The Commission should not adopt additional requirements that are so burdensome that they effectively eliminate the beneficial and properly supervised use of outside design firms, original equipment manufacturers ("OEMs"), and similar third-party vendors. The modern ICT ecosystem relies heavily on specialization, with different firms providing expertise in component development, engineering, manufacturing, branding, and distribution. Likewise, design houses and OEMs should continue to have the ability to market products through established brands and other partners. These "white labeling" arrangements promote competition, enable efficiencies throughout the supply chain, and ultimately provide consumers with lower costs and greater product choice.

As discussed above, the Commission can address legitimate provenance concerns without imposing additional disclosure obligations that would significantly diminish the benefits of these

arrangements and risk overwhelming the equipment authorization process. Rather than layering new reporting requirements onto existing authorization procedures, the Commission should focus on clearly identifying prohibited production activities involving Covered List entities and continue relying on its existing attestation framework within the equipment authorization process.[25] This targeted approach would more effectively address the Commission's concerns while preserving beneficial industry practices that have long supported innovation and competition.

b. *Importation Restrictions Should Primarily Focus on Producer/Provider-Based Covered List Equipment*

TIA supports the Commission imposing limitations on the importation of producer/provider-based Covered List equipment consistent with their underlying national security determinations. Because those restrictions identify specific entities, they reflect a reasonable extension of the Commission's existing Covered List framework.[26] The Commission should not, however, automatically apply those same restrictions to production location-based Covered List equipment. As discussed throughout these comments, production location-based determinations are fundamentally different in both scope and effect, often affecting broad categories of equipment and substantial portions of global supply chains. Applying identical importation restrictions in both contexts risks imposing significant burdens without a corresponding security benefit.

---

[25] *See eg. Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Report & Order, Order, and Further Notice of Proposed Rulemaking, ET. Doc. No. 21-232 at ¶¶ 52-58 (Nov. 11, 2022) (discussing adopting new attestation requirements).

[26] Even in the case of producer/provider-based categories, however, the Commission should consider allowing very small quantities of Covered List equipment to be imported under stringent conditions for an extremely narrow set of activities, such as tear downs that help guard against intellectual property theft and cybersecurity risks and allow for compatibility testing necessary to allow U.S. companies to continue to take the global lead on wireless innovations.

TIA is particularly concerned with the proposal to reduce testing and evaluation quantities from 4,000 units to 40 units per model.[27] Given the abrupt nature of Covered List additions, such a reduction could unnecessarily disrupt important testing, evaluation, and product-development activities. This concern is especially acute in light of the shifting scope and application of this year's production location-based prohibitions, where products may move from authorized status to Covered List restrictions and then authorization through a Conditional Approval within relatively short periods of time. If the Commission determines that stricter quantity limitations are necessary, such restrictions would be far more appropriately targeted to producer/provider-based Covered List determinations than to production location-based designations.

c. *The Commission Should Preserve Flexibility for Experimental and Pre-Authorization Activities*

The FCC seeks comment on whether existing exceptions for trade-show demonstrations and developmental, design, or pre-production evaluation should remain available for covered equipment.[28] TIA encourages the Commission to preserve these existing exceptions for trade-show demonstrations and developmental, design, and pre-production evaluation activities. Industry relies heavily on these pre-commercial phases to assess device performance, evaluate market demand, refine technical specifications, and develop business cases before committing the substantial resources necessary to obtain equipment authorizations and scale manufacturing operations. In many cases, manufacturers must invest significant resources before a product

[27] FNPRM at ¶ 161.
[28] FNPRM at ¶ 196.

reaches consumers, and those investments depend on the ability to conduct meaningful testing and demonstrations in realistic deployment environments.

While certain limitations may be workable in the context of producer/provider-based Covered List equipment, applying comparable restrictions to production location-based Covered List categories would be considerably more difficult and could impair product-development activities across broad segments of the industry. Companies need robust experimental and trial programs to validate products in the conditions under which they may ultimately be deployed. Requiring Commission approval for routine testing and evaluation activities would be administratively inefficient and could significantly chill innovation, particularly where manufacturers face uncertainty regarding whether entire categories of products may become subject to Covered List restrictions.

As the Commission evaluates even producer-based limitations on experimentation and development activities, it is worth noting that an overly strict limitation may inadvertently impede efforts to develop alternatives to covered equipment. Continued engagement in research, development, interoperability testing, and standards-related activities remains essential to maintaining a competitive communications ecosystem, even for producer-based equipment that is no longer authorized in the U.S. but used globally. The U.S. government has long recognized the importance of supporting appropriate engagement in international standards-development activities, even where participants may include entities subject to various restrictions.[29]

[29] *See e.g. Standards-Related Activities and the Ecport Administration Regulations*, Department of Commerce, Bureau of Industry and Security, Interim Final Rule, 15 CFR 734, 744, 772 (July 18, 2024) (*available at* https://www.federalregister.gov/documents/2024/07/18/2024-15810/standards-related-activities-and-the-export-administration-regulations).

Ultimately, the Commission can best advance its national security objectives by preserving the flexibility necessary for lawful product development, testing, manufacturing, and supply chain management while focusing restrictions on clearly identified risks.

VI. The Commission Should Emphasize Targeted Enforcement and Modern Compliance Tools

a. Streamlined Revocation Should Remain Focused on National Security Concerns and Material Misconduct

The FNPRM seeks comment on expanding the FCC's streamlined revocation procedures to equipment authorizations involving willful false statements, misrepresentations, or failures to provide required updates to the FCC, TCBs, DoW, or DHS.[30] TIA appreciates the Commission's efforts to ensure that it possesses effective tools to address threats to the integrity of the equipment authorization process. To that end, TIA does not object to streamlined revocation under these specific national security and deception-based circumstances.

At the same time, the Commission should maintain its existing revocation process for all other devices and scenarios. These existing Commission procedures already provide substantial safeguards, as the Commission already retains authority to set aside grants within 30 days following authorization, recently adopted streamlined procedures for covered equipment,[31] and other enforcement tools. Further, the Commission has developed a robust body of enforcement precedent that, thus far, has proven effective in deterring the violations of its equipment authorization rules. Taken together, these existing procedures provide the Commission with

[30] FNPRM at ¶¶ 182-186.
[31] *See e.g. Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Report & Order, Order, and Further Notice of Proposed Rulemaking, ET. Doc. No. 21-232 (Nov. 11, 2022)

substantial authority to address misconduct while preserving appropriate procedural protections for regulated entities.

b. *Modernization of the Equipment Authorization System Would Produce Greater Benefits than Introducing New Reporting Requirements*

Throughout this proceeding, TIA has encouraged the Commission to pursue solutions that improve compliance and enforcement while minimizing unnecessary burdens on industry. Consistent with that approach, TIA strongly supports modernization of the Equipment Authorization System ("EAS") and related Commission databases. In prior proceedings, TIA has urged the Commission to continue improving its digital databases and compliance systems to provide more user-friendly tools for manufacturers, retailers, certification bodies, and consumers.[32] We again urge the Commission to take this opportunity to modernize both the EAS and the Knowledge Database to better support compliance activities and improve access to information. The Commission should also take steps to ensure that these critical systems remain available and operational during lapses in federal appropriations, given the central role they play in equipment authorization and marketplace compliance.

Such updates should include modernized application programming interfaces ("APIs"), machine-readable authorization records, and similar capabilities that could significantly improve equipment authorization compliance and enforcement. These updated tools would allow regulated entities, certification bodies, online marketplaces, and enforcement personnel to more efficiently verify authorization information and identify compliance issues. More broadly, better data systems can achieve many of the Commission's stated objectives more effectively than expansive reporting obligations that require industry to submit and continually update large

[32] Comments of TIA, ET Doc. No. 24-136 (Jul. 15, 2026).

volumes of information. Finally, as the Commission contemplates potentially hosting an increasingly broad and critical scope of information from ICT manufacturers, it must take steps and spend additional resources to ensure its databases are hardened from potential cyber incursions that could create a national security risk greater than those the Commission seeks to mitigate through the collection of such data.

c. *Any U.S.-Based Liable Party Requirement Should be Carefully Evaluated and Include a Sufficient Transition Period*

TIA appreciates the Commission's interest in ensuring that there are effective mechanisms for enforcing compliance with the equipment authorization rules. While TIA does not strongly oppose a U.S.-based liable-party requirement in principle, the Commission should carefully evaluate the impacts of such a proposal based on the record developed in this proceeding. In particular, the Commission should consider how any new requirement would affect manufacturers, importers, retailers, distributors, and other lawful market participants that operate within the existing equipment authorization framework.

The Commission should also carefully evaluate how a new liable-party requirement would interact with current importer, distributor, retailer, and responsible-party obligations already embedded within the Commission's rules. Duplicative or overlapping responsibilities could create confusion while providing little additional enforcement benefit. Specifically, any new liable-party rules should explicitly recognize the distinct operational roles of authorization grantees and third-party contract manufacturers. Applying joint and several liability across all entities in the supply chain creates legal uncertainty and duplicates administrative burdens without delivering additional national security benefits. Should the Commission ultimately determine that a U.S.-based liable-party requirement is necessary to advance the public interest

and national security, any such requirement should be narrowly tailored to demonstrated enforcement concerns and implemented through an appropriate transition period.

To avoid such confusion, any new liable-party framework should recognize and preserve the distinct operational and regulatory roles of grantees and third-party contract manufactures. As the authorization holder, the grantee should retain primary authority over device design, component selection, and FCC compliance strategy without subjecting contract manufacturers to redundant regulatory oversight for builds executed strictly to grantee specifications. Conversely, where a contract manufacturer acts outside those specifications, such as introducing unauthorized component substitutions, regulatory accountability for that deviation should rest directly with the contract manufacturer rather than imposing joint liability or enforcement penalties on the good-faith grantee.

VII. The Commission Should Abandon Proposals that would Impose Significant Costs Without Corresponding Security Benefits

a. An Expanded FCC Logo Requirement would Provide Minimal Security Benefit

The FNPRM seeks comment on whether voluntary use of the FCC logo helps enforce the equipment authorization rules for SDoC devices currently eligible for its use and whether the logo should also be permitted or required for certified devices.[33] At this time, the Commission should decline to expand its FCC logo requirements absent a demonstrated showing that such requirements would materially improve compliance or advance national security objectives. As the FNPRM recognizes, certified devices already display an FCC ID, while devices authorized under the SDoC framework already are subject to FCC labeling rules.[34] These existing

[33] FNPRM at ¶¶ 177-181.
[34] *Id.*

requirements provide consumers, retailers, and enforcement personnel with information regarding a device's authorization status. The Commission has not demonstrated that additional logo requirements would meaningfully improve the effectiveness of this framework or address any identified national security concern.

Furthermore, imposing a requirement to display an FCC logo on certified devices would reimpose burdens eliminated in the first Trump Administration, in contravention of the goals of the Commission's Delete proceeding. At present, display of the FCC logo is not required on any FCC-authorized devices. Pre-2017 devices authorized via older Declaration of Conformity procedures were required to display the FCC logo. In 2017, however, the use of the FCC logo became voluntary for SDoC devices after the Commission found that "continuing to require the FCC logo would create an unnecessary burden on device manufacturers."[35] That statement remains true. Additional burdens could also arise from customer confusion, as numerous devices of different vintage (i.e., those authorized using pre-2017 procedures, those authorized between 2017 and the effective date of any new rules, and those authorized after new rules go into effect) could remain in the marketplace, all following different and valid regulations for displaying the FCC logo.

Compliance with existing FCC labeling obligations already consumes a significant portion of available device labeling and packaging space, particularly for smaller and consumer-oriented devices. At the same time, the Commission's current approach does not fully reflect modern methods of providing regulatory information, including the broader use of QR codes, electronic labeling, and other digital disclosure tools. Rather than expanding existing logo

[35] *Amendment of Parts 0, 1, 2, 15, and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, First Report & Order, ET Doc. No. 15-170, at ¶ 18 (Jul. 13, 2017).

requirements, the Commission should continue exploring ways to modernize its labeling framework so that required information remains accessible while reducing unnecessary burdens on manufacturers. Without further modernization of the Commission's labeling requirements, any additional labeling obligations border on infeasible and merely increase compliance burdens without producing meaningful security gains.

b. *Equipment Authorization Term Limits Would Create Significant Administrative Burdens Without Corresponding Security Benefits*

TIA likewise opposes the imposition of expiration dates or term limits on existing equipment authorizations.[36] Such a requirement would generate significant and unnecessary burdens for both equipment manufacturers and the Commission without any demonstrated corresponding improvement in national security outcomes. The Commission has not established a clear connection between equipment authorization expiration dates and the national security concerns underlying the Covered List. Equipment that complies with the Commission's rules does not become less compliant merely because an authorization has existed for a certain number of years. Nor has the Commission demonstrated that requiring periodic reauthorization would provide meaningful insight into whether a device incorporates covered equipment or is otherwise subject to Covered List restrictions.

By contrast, authorization term limits would require manufacturers to devote substantial resources toward renewing authorizations for existing products and would likely generate a significant volume of additional filings for Commission staff to review. The cost of this administrative burden would be borne not only by industry and, ultimately, consumers, but also by Commission staff who would be required to process large numbers of renewal applications

[36] FNPRM at ¶¶ 208-210.

that may present few, if any, substantive compliance issues. These are just the kind of results that the Commission's bold actions in its Delete docket were meant to curtail. The resources that would be needed to obtain renewals of authorizations would be better directed toward improving product security, maintaining compliance with existing requirements, addressing emerging threats, and bringing innovative new technologies to market. If the Commission nevertheless adopts a term limit requirement, such a requirement should only apply to prospective devices. The Commission should not retroactively apply a timeline to grants that were made without a timeline, as such a decision would apply a recission of terms granted by the FCC that manufacturers have relied on and could interfere with the continued operation of devices already in use. In setting forth a renewal requirement, the Commission also should make clear what rules would guide any analysis (i.e., those regulations in effect at the time of the original grant or subsequent updates) and explain the consequences for non-renewal for those devices already manufactured deployed in the marketplace.

VIII. Conclusion

TIA appreciates the Commission's continued efforts to protect U.S. communications networks from threats posed by foreign adversaries and to promote trusted ICT manufacturers through exercise of its authority under the Secure Networks Act and Secure Equipment Act. As the Commission evaluates the proposals raised in the FNPRM, it should remain mindful that the Covered List is most effective when its restrictions are closely tied to the specific national security determinations that gave rise to a listing and tailored to the risks those determinations seek to address.

Accordingly, TIA urges the Commission to continue distinguishing between producer/provider-based and production location-based Covered List determinations, preserve

the flexibility necessary for innovation and supply chain resiliency, and focus on targeted enforcement and modernization of existing compliance tools rather than imposing broad and administratively burdensome new reporting and authorization requirements that would transform the entire ICT equipment authorization program. We look forward to continuing to work with the Commission on policies that strengthen U.S. networks, promote trusted communications infrastructure, and ensure that the equipment authorization process remains efficient, predictable, and effective in furtherance of the public interest.

_/s/_____
Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard, Floor 9
Arlington, VA 22209

September 8, 2026