

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

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

REPLY COMMENTS OF INCOMPAS

INCOMPAS

Staci L. Pies
Senior Vice President, Government
Relations and Policy
1100 G Street, N.W., Suite 800
Washington, DC 20005
spies@incompas.org

September 28, 2026

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	THE RECORD CONFIRMS THAT COVERED LIST IMPLEMENTATION MUST REMAIN TIED TO SPECIFIC NATIONAL SECURITY DETERMINATIONS	2
A.	The Commission Should Not Convert Its Implementation Role into General Supply Chain Authority	2
B.	The Record Supports the Logic-Bearing or Distinct RF Nexus Boundary	5
C.	Any Definition of “Produced By” Must Turn on Ongoing Control over Security-Critical Functions.....	7
D.	The Record Supports Rejecting a Universal HBOM and SBOM Filing Mandate.....	8
1.	Commenters Across the Affected Supply Chains Identify Fundamental Defects in the Commission’s Proposals	8
2.	Commenters Supporting Broad Disclosure Do Not Justify a Universal Filing Rule.....	10
3.	If the Commission Proceeds, Any Requirement Must Preserve Essential Statutory and Risk-Based Limits.....	11
III.	THE RECORD DOES NOT SUPPORT SECTOR-WIDE CERTIFICATION OR UNIVERSAL SDoC REGISTRATION	13
A.	The Commission Should Not Require Certification Solely Because Equipment Falls Within a Covered List Sector	13
B.	Universal SDoC Registration Would Create New Burdens Without Verifying Compliance or Enabling Marketplace Verification	15
IV.	THE COMMISSION SHOULD REJECT THE FORTY-UNIT IMPORTATION LIMIT AND PRESERVE WORKABLE TESTING, EVALUATION, AND R&D PATHWAYS.....	18
V.	THE COMMISSION SHOULD NOT APPLY A SINGLE OVERBROAD DEFINITION OF “PRODUCED IN A FOREIGN COUNTRY” ACROSS COVERED LIST SECTORS	20
VI.	THE COMMISSION SHOULD REJECT UNIVERSAL TERM LIMITS AND PRESERVE PROCEDURAL SAFEGUARDS.....	22
A.	The Commission Should Reject Fixed Terms for Equipment Authorization	22
B.	Any Expedited Revocation Process Must Preserve Procedural Safeguards	24
VII.	CONCLUSION	25

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

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

REPLY COMMENTS OF INCOMPAS

I. INTRODUCTION AND SUMMARY

INCOMPAS members build and operate the infrastructure that supports U.S. leadership in AI and other advanced technologies. Their fiber and wireless networks connect users, cloud regions, and data centers, while their communications and computing services support the facilities where AI systems are trained and deployed. Members are investing substantially in the equipment needed to expand that infrastructure. Rules governing the authorization, importation, testing, and marketing of such equipment therefore directly affect the cost and pace of AI and communications deployment.

INCOMPAS members also have a direct interest in a secure equipment ecosystem. Compromised equipment can threaten network reliability and critical services, while uncertainty about which products are trustworthy can delay investment and deployment. INCOMPAS therefore supports targeted action against clearly identified national-security threats, including measures that prevent evasion of Covered List restrictions and help companies avoid covered equipment. Well-designed protections strengthen the infrastructure that underpins American technological leadership and economic growth.

Congress established a deliberate division of responsibility. The national-security sources named in the Secure Networks Act identify equipment or services that pose an unacceptable risk, while the Federal Communications Commission (“Commission” or “FCC”) carries those determinations into the Covered List and equipment-authorization program. This structure places threat assessment with the agencies Congress selected for that task and leaves implementation to the Commission. The FCC should not use its implementing authority to enlarge a determination or make a national-security judgment assigned to another source.

The record reflects broad agreement that secure supply chains do not require universal reporting, registration, certification, or expiration mandates that are not tied to an identified risk. Commenters representing manufacturers, network operators, technology companies, and downstream sellers repeatedly explain that such mandates would require information that responsible parties may not possess or be able to verify. They would also delay trusted products and redirect engineering and compliance resources away from measures responsive to demonstrated vulnerabilities and from the infrastructure investment needed for American leadership in AI and advanced technologies.

The Commission should reject adoption of those universal mandates and preserve existing authorization and development pathways for equipment not covered. If the Commission nevertheless considers a narrower requirement, it must identify the statutory authority and the specific risk supporting the rule, tie the obligation to the applicable national-security determination, and account for the regulated party's practical ability to obtain and verify the required information. These alternative limitations do not endorse a new mandate; they preserve INCOMPAS and its members' ability to address a narrower Commission approach as the record develops.

II. THE RECORD CONFIRMS THAT COVERED LIST IMPLEMENTATION MUST REMAIN TIED TO SPECIFIC NATIONAL SECURITY DETERMINATIONS

A. The Commission Should Not Convert Its Implementation Role into General Supply Chain Authority

Congress assigned different responsibilities to different institutions. The Commission has repeatedly acknowledged that its role under the Secure Networks Act is to publish, update, and implement the Covered List based on qualifying determinations made by designated national-security sources. The FCC does not independently reassess the identified threat, disregard or modify the source's judgment, or add equipment to the Covered List on its own initiative. Once a designated source makes a qualifying determination, the Commission must implement it according to its terms.¹

¹ See 47 U.S.C. § 1601(a)–(d); 47 CFR §§ 1.50002(a)–(b), 1.50003; *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14316, 14318–19, 14324–25, paras. 71, 74–76, 89, 91 (2020) (*Supply Chain Second Report and Order*) (explaining that the Commission does not independently assess the national-security threat identified by an enumerated source, has no discretion to disregard or modify the source's determination, and performs a nondiscretionary, ministerial function when publishing and updating the Covered List); *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, ET Docket No. 21-232, Third Report and Order and Third Further Notice of Proposed Rulemaking, FCC 26-50, at 17, para. 36 (July 23, 2026) (*Third R&O* and *Third FNPRM*, respectively) (“The Commission lacks the authority to add to the Covered List on its own initiative.”), corrected by Erratum, DOC-424161A1 (OET Aug. 13, 2026); *China Unicom (Americas) Operations Limited*, WC Docket No. 18-89, Order on Reconsideration, 40 FCC Rcd 3335, 3342–45, paras. 18, 21–22, 26 (PSHSB 2025) (*China Unicom Reconsideration Order*) (explaining that the Commission may not disregard a determination from an enumerated source, does not conduct a separate national-security or capability analysis when that source has performed the required analysis, and acts in a nondiscretionary, ministerial capacity when updating the Covered List).

The Commission’s implementation role is important but bounded: it carries out the qualifying determination; it does not create a new covered class of equipment, components, or entities that the designated source did not identify. INCOMPAS, the Telecommunications Industry Association (“TIA”), the Information Technology Industry Council (“ITI”), CTIA, and the Computer & Communications Industry Association (“CCIA”)—trade associations representing a broad and diverse cross-section of the communications and technology ecosystem, including network operators, equipment manufacturers, fiber and wireless providers, and technology, cloud, and internet companies—converge on the same central point: Congress authorized the Commission to implement qualifying national-security determinations made by designated sources, not to impose universal requirements untethered to those determinations.²

INCOMPAS’s initial comments explain why the Secure Networks Act, the Secure Equipment Act, section 302(a) of the Communications Act, and the Commission’s ancillary authority do not authorize a universal supply-chain provenance mandate. The Foundation for Defense of Democracies (“FDD”), a national-security and foreign-policy research institute, takes a broader view. But FDD’s invocation of national-security concerns, the Secure Networks Act, the Secure Equipment Act, and *Huawei* does not identify statutory language authorizing the Commission to require every equipment-authorization applicant to report the producer, production location, and country-value share of every lower-tier component, including for devices with no demonstrated nexus to an applicable Covered List entry. Those authorities permit the Commission to implement qualifying national-security determinations; they do not independently authorize a universal component-provenance reporting regime untethered to such a determination.³

Nor does the decision in *Huawei Technologies USA, Inc. v. FCC* supply the missing authority. *Huawei* reviewed an FCC rule prohibiting universal-service support recipients from using FCC-administered subsidies to purchase equipment or services from companies designated as national-security risks. The Fifth Circuit upheld that rule based on section 254(c)(1)(D), read together with section 201(b), and section 254(b)(1), concluding that those provisions permitted the Commission to exercise limited national-security judgment when administering the Universal Service Fund. The court did not hold that a general national-security interest creates freestanding Commission jurisdiction. To the contrary, it rejected the premise that the absence of an express statutory prohibition can itself establish agency authority and

² INCOMPAS Comments at 1–3, 7–8, 25–26; TIA Comments at 4–12; ITI Comments at 2–5; CTIA Comments at 12–18; CCIA Comments at 3–4, 8–10.

³ Foundation for Defense of Democracies Comments at 2, 4–6 (FDD Comments); 47 U.S.C. § 1601(a), (c); Secure Equipment Act of 2021, Pub. L. No. 117-55, § 2(a)(2), 135 Stat. 423, 423–24 (codified at 47 U.S.C. § 1601(d)(2)); INCOMPAS Comments at 1–3, 7–8, 25–26.

emphasized that the authority before it was “limited” and tied to the Commission’s administration of universal service. Although the court referred to section 303’s “public interest” language in interpreting the provisions before it, it did not decide whether sections 302 or 303 authorize requirements under the equipment-authorization program, much less universal component-provenance filings. *Huawei* therefore does not establish Commission authority for the mandate proposed here.⁴

The Commission’s remaining authorities do not fill that gap. In adopting its logic-bearing-hardware rule, the Commission invoked sections 302(a), 303(e), 303(g), and 303(r) of the Communications Act, together with section 4(i), the national-defense and public-safety purposes stated in section 1, and provisions of the Communications Assistance for Law Enforcement Act. Those provisions must be considered on their actual terms. Sections 302(a) and 303(e) and (g) authorize regulation of radiofrequency (“RF”) devices, radio apparatus, and effective spectrum use; sections 4(i) and 303(r) permit measures ancillary to responsibilities conferred elsewhere; section 1 states statutory purposes; and CALEA addresses carriers’ lawful-interception obligations. Even if those provisions support targeted requirements for equipment or components with a direct RF or qualifying Covered List nexus, the Commission must identify how each element of a universal lower-tier provenance filing is necessary to an assigned statutory function. General national-defense, public-interest, and ancillary-authority provisions do not themselves create freestanding jurisdiction over every supplier and production location in a device’s supply chain. That limitation is especially important after *Loper Bright Enterprises v. Raimondo*: statutory ambiguity is not itself a delegation of authority, and a reviewing court must independently determine whether an agency has acted within the authority Congress conferred. The Commission therefore has not identified a statutory basis for the universal mandate proposed here.⁵

The distinction between implementing a qualifying national-security determination and creating a new class of covered equipment has practical consequences for companies investing in digital infrastructure. Equipment decisions are made well before deployment and often shape the design of the larger system. If the Commission treats a trusted finished device as prohibited when no qualifying determination reaches that device, it could strand investment and delay deployment without any finding that the equipment presents an unacceptable national-security risk. The Commission therefore must identify

⁴ *Huawei Technologies USA, Inc. v. FCC*, 2 F.4th 421, 426–27, 436, 439–47 (5th Cir. 2021); *Third R&O* at 9, para. 19 & nn.44–49.

⁵ See 47 U.S.C. §§ 151, 154(i), 229(a)–(b), 302a(a), 303(e), (g), (r); 47 U.S.C. § 1004; *Third R&O* at 9, para. 19 & nn.44–49; *Third FNPRM* at 49–51, paras. 139–46; *American Library Ass’n v. FCC*, 406 F.3d 689, 698–700, 708 (D.C. Cir. 2005); *Comcast Corp. v. FCC*, 600 F.3d 642, 655–61 (D.C. Cir. 2010); *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948–50 (D.C. Cir. 2024); *Loper Bright Enterprises v. Raimondo*, 603 U.S. 369, 399–401, 412–13 (2024).

the qualifying determination before extending an authorization prohibition and apply that prohibition only to equipment within the determination's actual scope.

B. The Record Supports the Logic-Bearing or Distinct RF Nexus Boundary

The *Third Report and Order* prohibited authorization of a device containing a logic-bearing hardware component produced by a Covered List entity when the device would be prohibited if that entity had produced the finished device. At the same time, the Commission declined to adopt broader restrictions unsupported by a specific national-security determination and declined to extend the prohibition to all components, software, or firmware. The *Third FNPRM* now asks whether the Commission should prohibit authorization of devices containing any component produced by a Covered List entity, including passive components, or software or firmware produced or provided by such an entity. INCOMPAS and commenters across the communications and technology sectors oppose that general expansion and explain that any component restriction must remain tied to an identified risk and the scope of a qualifying national-security determination.⁶ SAFE likewise urges the Commission to focus on security-relevant components and exclude passive or de minimis parts absent a demonstrated nexus to risk.⁷

INCOMPAS urges the Commission to retain the functional boundary identified in its initial comments. Unless a qualifying national-security determination specifically reaches additional components or functionality, any further restriction should remain limited to logic-bearing hardware components or components with a distinct nexus to RF communications. Even then, a component should affect authorization of the finished device only when the component, its producer, and the relevant risk fall within the scope of the applicable determination. Passive or ordinary mechanical parts should not cause a device to lose authorization merely because they appear somewhere in a multi-tier supply chain. Software and firmware require the same determination-specific analysis. The presence of a particular software package does not establish, standing alone, that an enumerated source has determined that the finished device presents an unacceptable risk or constitutes covered equipment.

The Coalition for a Prosperous America ("CPA"), which describes itself as a bipartisan coalition of manufacturers, workers, and agricultural producers, raises a specific concern about optical transceivers used in data centers. It asks an enumerated national-security source to determine whether transceivers produced by certain named suppliers should be covered. CPA also urges the Commission to adopt universal HBOM and SBOM filings and prohibit authorization of devices containing any component produced by a

⁶ See *Third R&O* at 8–10, 14, paras. 16, 20–23, 29–30; *Third FNPRM* at 51–53, paras. 147–52; INCOMPAS Comments at 14–19; ITI Comments at 10–12; CTIA Comments at 22–23; TIA Comments at 10–12; CCIA Comments at 8–10; Faraday Comments at 3–4.

⁷ Comments of the Secure and Advanced Non-FEOC Energy Alliance at 1, 6–7 (SAFE Comments).

Covered List entity. Those broader recommendations do not follow from the transceiver-specific concern CPA identifies. Evidence concerning one class of logic-bearing modules does not establish the necessity, legal authority, or workability of rules governing every component in every device submitted for authorization.⁸

This rulemaking is not a substitute for the predicate determination required by the Secure Networks Act. An enumerated national-security source must evaluate the asserted risk and identify the equipment or services reached by its determination. Only after that process is complete may the Commission publish and implement the resulting Covered List entry, and the Commission must adhere to the determination's actual terms. It should not prejudice the source's assessment or treat CPA's allegations as though the required determination had already been made.⁹

Recognition of that statutory process does not mean that INCOMPAS supports adding optical transceivers to the Covered List. Optical transceivers are essential to the data-center and high-capacity network infrastructure that supports cloud computing and AI. An overbroad restriction could make essential equipment more difficult and expensive to obtain, slowing infrastructure deployment and disrupting established supply chains and trade.¹⁰ Before issuing any determination, the responsible national-security source should establish a sound factual basis for the asserted risk and define precisely the equipment and suppliers that would fall within its scope. It also should assess whether trusted alternatives can be qualified in time to avoid unnecessary harm to infrastructure deployment and broader economic security, including competition and trade. To the maximum extent consistent with protecting classified or otherwise sensitive information, affected parties should have a meaningful opportunity to provide relevant technical and supply-chain evidence.

Even if an enumerated source later issues a qualifying determination addressing specified optical transceivers, that determination would not establish a basis for an industry-wide component prohibition or a universal reporting mandate. Any Commission action would have to remain within the determination's actual terms and the authority Congress conferred. A determination addressing particular transceivers or producers would not justify prohibiting unrelated components incorporated into other equipment or requiring every certification applicant to submit universal Hardware Bill of Materials ("HBOM") and

⁸ Comments of the Coalition for a Prosperous America at 1–2 (CPA Comments); see *Third FNPRM* at 49–53, paras. 139–45, 147–52.

⁹ See 47 U.S.C. § 1601(a)–(c); *Third R&O* at 17, para. 36; *China Unicom Reconsideration Order*, 40 FCC Rcd at 3342–45, paras. 18, 21–22, 26.

¹⁰ See INCOMPAS Comments at 2–3; CPA Comments at 1–2 (describing the role of optical transceivers in AI data centers and citing potential constraints on alternative supply).

Software Bill of Materials (“SBOM”) filings. The record in this proceeding does not support rules of general application extending authorization prohibitions beyond logic-bearing hardware components or components with a distinct nexus to RF communications without a specific national-security determination reaching those additional components.

C. Any Definition of “Produced By” Must Turn on Ongoing Control over Security-Critical Functions

The proposed “any major stage” standard is too vague for equipment-authorization applicants, Telecommunication Certification Bodies (“TCBs”), and the Commission to apply consistently. ITI, CTIA, and TIA generally support codifying a definition of “produced by,” but ask the Commission to exclude ordinary licensing, standards participation, routine supply relationships, and historical design contributions that do not confer continuing authority over the device. CCIA more directly objects that “any major stage” leaves applicants without a discernible line. The qualifications requested even by commenters otherwise supportive of codification confirm the same problem: participation in one step of a multi-tier development process does not establish responsibility for the finished model or its security posture.¹¹

The statutory framework supplies the necessary limiting principle. Where a Covered List entry reaches equipment “produced by” a named entity, the Commission may interpret that phrase to prevent the entity from evading the determination by selling the same device under another company’s brand. It may not define the phrase so broadly that the implementing rule reaches entities or equipment outside the source determination. Otherwise, the Commission’s definition, not the national-security source’s determination, would establish the scope of the prohibition.

INCOMPAS therefore proposes a model- and version-specific inquiry focused on present authority over the device submitted for authorization. An entity should be treated as a producer only when it exercises exclusive or primary ongoing control over a security-critical function of that model or holds exclusive authority over its final manufacturing specifications. Relevant control may include authority over firmware compilation and signing, secure-boot protections, update pathways, or cryptographic credentials. Separate security-critical functions must be assessed separately: two entities cannot each exercise exclusive control over the same function, although different entities may independently satisfy the standard with respect to distinct functions.

¹¹ INCOMPAS Comments at 19–24; ITI Comments at 5–7; CTIA Comments at 10–12; TIA Comments at 8–9; CCIA Comments at 4–6; CTA Comments at 21–23; NAM Comments at 3; Ciena Comments at 11–12; *Third FNPRM* at 46–47, paras. 130–35.

By contrast, merely supplying a component, licensing preexisting intellectual property, contributing to a technical standard, assembling a device under another party’s specifications, or participating in development of a predecessor model should not confer producer status by itself. Historical design involvement also should not determine the producer of a later model after another company has assumed the relevant ongoing control. These exclusions are necessary to give applicants fair notice and to prevent the term “producer” from expanding to every participant in an extended supply chain.

The same limit should govern the proposed signed list of “any and all” producers. An applicant should identify entities that it knows, after reasonable diligence, independently satisfy the final control standard; it should not be required to guarantee that the Commission will never characterize a remote contributor’s earlier work as a major stage of production. This approach addresses genuine white-label evasion while aligning responsibility with the entities that can determine or materially alter the security-critical implementation of the authorized device.

D. The Record Supports Rejecting a Universal HBOM and SBOM Filing Mandate

1. Commenters Across the Affected Supply Chains Identify Fundamental Defects in the Commission’s Proposals

The record contains substantial opposition to requiring every certification applicant to file an HBOM and an SBOM. ITI, CTIA, TIA, CCIA, the Semiconductor Industry Association (“SIA”), Faraday, Boston Dynamics, CEDIA, and other affected commenters either oppose universal submission or describe information they cannot obtain and maintain as proposed.¹² SAFE and Humanoid support proportionate measures aimed at security-relevant components.¹³ Those comments supply operational evidence; they should not be mistaken for opposition to knowing whether equipment actually falls within a Covered List entry.

A manufacturer often knows its direct suppliers but lacks verified information about entities several tiers removed from the finished device. The *Third FNPRM* would require producer and production-location data and allocations of component value by location, as well as updates within 30 days of any material change. Conventional SBOM formats identify software components and dependencies; they do not themselves establish the country in which each component was developed or allocate value among countries. Sourcing changes and software updates could leave a filed artifact stale or turn a one-time

¹² INCOMPAS Comments at 24–33; ITI Comments at 7–10; CTIA Comments at 18–22; TIA Comments at 13–20; CCIA Comments at 6–8; Semiconductor Industry Association Comments at 3–8 (SIA Comments); Boston Dynamics Comments at 6–8, 13–14; Faraday Comments at 3–4; CEDIA Comments at 2–3; CTA Comments at 28–35; Ciena Comments at 3–11.

¹³ SAFE Comments at 5–6; Humanoid Comments at 8–9.

application into recurring submissions. The Commission has not shown how an applicant could certify that the proposed lower-tier fields are accurate across that lifecycle.

The record demonstrates that the Commission's assumptions do not reflect the practical realities across affected technologies. SIA explains that semiconductor companies generally lack access to complete lower-tier provenance information and may substitute functionally equivalent chips during a product's lifecycle.¹⁴ Boston Dynamics likewise explains that automated SBOM generation would not be simple or costless for its systems: it estimates that developing the necessary tooling would require one or two engineers for most of a year and an initial investment of at least \$750,000 to \$1 million.¹⁵ Although the precise burden will vary by product and manufacturer, this evidence undermines any assumption that automation would make compliance uniformly straightforward or negligible.

As INCOMPAS explained in its initial comments, the proposed mandate also raises fundamental confidentiality concerns that implementation alone cannot resolve. A comprehensive HBOM or SBOM can reveal proprietary product architecture, software dependencies, supplier relationships, sourcing strategies, and potential points of attack. Public disclosure could cause competitive and security harm, while concentrating the same information in a centralized nonpublic repository would create a high-value target for attempted cyber intrusion or hacking. The Commission should not require companies building and supplying critical communications, advanced technologies, and AI infrastructure to create a new security vulnerability as the price of obtaining equipment authorization.

Sections 0.457(d), 0.459, and 0.461 of the Commission's rules provide procedures for protecting qualifying commercial information and addressing requests for disclosure,¹⁶ but case-by-case confidentiality requests do not answer whether a universal collection is justified or provide the categorical assurance that a mandatory repository would require. Any alternative collection must remain outside the public Equipment Authorization System record, receive legally enforceable nonpublic treatment subject only to disclosure required by law, and be accessible only to personnel with a demonstrated need for the information. If the Commission cannot provide that assurance, it should not require the filing. Submission to a Telecommunication Certification Body ("TCB") would not cure the problem unless the same enforceable confidentiality, access-control, and cybersecurity protections apply to that recipient.

¹⁴ SIA Comments at 3–4.

¹⁵ Boston Dynamics Comments at 7.

¹⁶ 47 CFR §§ 0.457(d), 0.459, 0.461.

2. Commenters Supporting Broad Disclosure Do Not Justify a Universal Filing Rule

Commenters supporting broader disclosure may identify legitimate security objectives, but they do not establish that the *Third FNPRM*'s universal remedy is necessary, accurate, or administrable. None bridges the gap between information that may be useful in a targeted security inquiry and a signed, continuously updated provenance filing for every certification application. Nor do they show that the Commission can make sensitive submissions useful to purchasers while providing the nonpublic treatment that the information requires. The Commission should evaluate each argument against the scope of the rule actually proposed.

NTCA–The Rural Broadband Association presents a legitimate concern on behalf of smaller network providers that may lack the purchasing leverage to obtain useful component information from vendors.¹⁷ Reliable software-component information can help providers identify and respond to known vulnerabilities, and INCOMPAS shares NTCA's interest in secure rural networks and predictable access to trusted equipment. Notably, NTCA also warns that broad certification requirements and equipment delays can harm also those providers. But NTCA's purchaser-side need for useful vulnerability information does not establish that every certification applicant should submit the substantially broader provenance data proposed in the *Third FNPRM*.

The FCC's proposed mandate would require signed HBOM and SBOM submissions identifying component producers, production locations, and the percentage of component value attributable to each producer and production location, followed by updates within 30 days of any material change.¹⁸ An applicant may know more about its finished product than a purchaser does and still lack a reliable means to verify facts held by remote suppliers. Filing those details with the Commission also would not necessarily make them available to NTCA's members because the commercially and security-sensitive information would require nonpublic treatment. NTCA identifies a real network-security need but does not show that the *Third FNPRM*'s universal provenance database would meet it. The mismatch instead reinforces INCOMPAS's position that the Commission should distinguish customer-useful vulnerability information from the detailed component-level supply-chain filing proposed here.¹⁹

¹⁷ NTCA–The Rural Broadband Association Comments at 1–4, 6–7, 11–15 (NTCA Comments).

¹⁸ See *Third FNPRM* at 50, para. 142 & App. B (proposing 47 CFR §§ 2.911(d)(9)–(10), 2.931(f)).

¹⁹ NTCA Comments at 11–15; *Third FNPRM* at 50–51, paras. 142–45.

Modgud Laboratories LLC, an Austin-based laboratory that describes experience examining electronic hardware, proposes pairing bills of materials with physical provenance verification.²⁰ Its concern that supplier information may be inaccurate reinforces INCOMPAS's objection to requiring applicants to certify facts they cannot independently verify. Modgud describes inspection techniques that may assist in examining a particular device, but its filing does not demonstrate that those techniques can identify every component producer and production location, or determine the percentage of each component's value associated with each production location, across the full range and volume of equipment subject to certification. It also does not supply an administrable framework for testing standards, accreditation, capacity, cost, or protection of the sensitive information revealed through examination. The possibility of investigating a suspect device does not justify mandatory physical verification for all applicants.

CPA and FDD likewise leap from asserted security concerns to rules of general application without establishing the need for that step. As discussed above, CPA asks an enumerated national-security source to assess specified optical transceivers and named suppliers.²¹ That request confirms that a designated source, not the Commission acting in this equipment-authorization rulemaking, must make the predicate risk determination. The Commission should not impose universal HBOM and SBOM filings either to prejudge that assessment or to assemble a record that the designated source, not individual applicants, must evaluate. FDD similarly supports comprehensive component reporting but does not establish why devices with no identified nexus to a Covered List determination should bear the same obligation.²² A targeted allegation cannot supply the legal or factual basis for a universal provenance regime.

None of these arguments resolves the *Third FNPRM* proposal's central defects: applicants may not possess or be able to verify the required lower-tier information; the submissions could become obsolete as products and sourcing change; and the confidentiality required to protect the data would limit its usefulness to the purchasers invoked in support of collection. The Commission should reject the universal HBOM and SBOM mandate and Modgud's proposed universal physical-verification regime.

3. If the Commission Proceeds, Any Requirement Must Preserve Essential Statutory and Risk-Based Limits

The record does not support adoption of a mandatory HBOM or SBOM filing rule, much less a universal requirement imposed on every certification applicant. Commenters across affected sectors

²⁰ Modgud Laboratories LLC Reply at 1–4 (Modgud Reply); *Third FNPRM* at 50–51, paras. 142–46.

²¹ CPA Comments at 1–2; FDD Public Comment at 2, 4; 47 U.S.C. § 1601(c); *Third FNPRM* at 49–53, paras. 139–45, 147–48.

²² NTCA Comments at 1–4, 6–7, 11–15; Modgud Reply at 1–4; CPA Comments at 1–2; FDD Public Comment at 2, 4–5; *Third FNPRM* at 49–53, paras. 139–48.

demonstrate that such a mandate would require applicants to submit information they often do not possess and cannot independently verify, impose substantial burdens without a demonstrated connection to an identified risk, and concentrate sensitive commercial and security information in a government repository. INCOMPAS therefore urges the Commission to reject the proposal. If the Commission nevertheless proceeds, the limitations below define the outer bounds of any disclosure requirement consistent with the record and the applicable statutory framework.

At the device level, any disclosure requirement must be confined to a clearly defined, higher-risk subset of equipment supported by an evidence-based assessment of an identified supply-chain or national-security risk and consistent with the applicable national-security determination. A device's presence within a sector addressed by a Covered List entry may be relevant only where the underlying determination makes component origin material. Sector membership alone should not trigger disclosure, alter the device's otherwise applicable authorization pathway, or create a presumption that the device falls within the Covered List entry. If addressing additional equipment would require expanding the underlying determination, that judgment must be made by an enumerated national-security source through the process Congress prescribed—not by the Commission through an implementing rule.

Within that limited device universe, any required disclosure must be confined to critical components or components having a distinct nexus to the provision of RF communications. The components subject to disclosure must be defined by reference to the particular risk identified in the applicable national-security determination. Applicants should be required to exercise reasonable diligence and permitted to rely on supplier representations unless they know, or have a reasonable basis to believe, that the information is materially inaccurate. An applicant's certification should attest to the information reasonably available through that process; it should not become a guarantee of information held by remote suppliers outside the applicant's knowledge or control.

Any disclosure requirement must provide legally enforceable protection for confidential commercial, proprietary, supply-chain, and security-sensitive information; harmonize its terminology and required fields with established federal and industry standards; apply prospectively; grandfather existing authorizations absent a qualifying determination addressing the affected equipment; and provide sufficient implementation time to establish supplier-reporting arrangements, internal controls, and secure submission processes. The Commission should not require submission of sensitive information unless it can assure nonpublic treatment, subject only to disclosure required by law. Requiring applicants to submit the same information to a TCB would not resolve the confidentiality or security concerns unless equivalent, legally enforceable protections, access restrictions, retention limits, and information-security safeguards apply to that recipient.

III. THE RECORD DOES NOT SUPPORT SECTOR-WIDE CERTIFICATION OR UNIVERSAL SDOC REGISTRATION

A. The Commission Should Not Require Certification Solely Because Equipment Falls Within a Covered List Sector

A Covered List entry reaches an entire sector only if the underlying qualifying determination defines the covered equipment that broadly. Each entry instead applies according to its own terms, which may depend on the producer, production location, or function of the equipment. A device that falls outside those terms is not covered merely because it belongs to the same industry sector or product category.²³

The *Third FNPRM* nevertheless proposes to use membership in a newly defined “Covered List sector” as the trigger for certification. Every device within such a sector would be required to obtain authorization through certification, even if the device is not covered equipment and otherwise qualifies for authorization through the Supplier’s Declaration of Conformity (“SDoC”) process or is exempt from equipment authorization. The proposal would therefore impose heightened treatment based on a category label rather than a determination that the particular device falls within a Covered List entry. That result departs from the determination-based structure Congress established through the Secure Networks Act and the Secure Equipment Act. Commenters across the communications and technology sectors explain in the record in this proceeding that sector membership neither establishes that a particular device presents the identified risk nor justifies eliminating authorization pathways that otherwise apply.²⁴

The Commission grounds its proposal in the additional oversight provided through applicant attestations, supporting documentation, and review by a Telecommunication Certification Body (“TCB”). It also identifies a potential gap involving host devices that incorporate previously authorized modular transmitters and may not require a separate authorization. Neither rationale supports the proposal’s full reach. Certification may facilitate review of information submitted in an application, but it cannot supply a national-security determination that does not cover the device. And the host-device concern involves a particular equipment configuration. The *Third FNPRM* does not explain why a rule directed to that configuration would be inadequate or why every non-covered product in the sector must undergo certification to address it.²⁵

²³ See 47 U.S.C. § 1601(a)–(c); 47 CFR § 1.50002(a)–(b); *Third R&O* at 17, para. 36.

²⁴ See 47 U.S.C. § 1601(a)–(c); Secure Equipment Act of 2021, Pub. L. No. 117-55, § 2(a)(2), 135 Stat. 423, 423 (2021); *Third FNPRM* at 54, paras. 153–54 & App. B (proposing 47 CFR §§ 2.902, 2.906(d), 2.907(c), 15.101(f)); CTIA Comments at 23–24; TIA Comments at 21–23; ITI Comments at 12–14; CCIA Comments at 10–12.

²⁵ See *Third FNPRM* at 54–55, paras. 153–56.

The power-inverter comments demonstrate the consequences of that overbreadth. The applicable national-security determination, as modified, does not cover every power inverter. It reaches utility-interactive inverters with specified remote-communication capabilities that are “foreign-produced” under the determination. An inverter is not treated as foreign-produced if it is eligible for the section 45X advanced manufacturing production credit for domestic production or qualifies as a domestic end product under 48 CFR § 25.101(a). The modified determination thus draws a line within the power-inverter category: some inverters are covered, while others are not.

TMEIC Corporation Americas (“TMEIC”), a producer of utility-scale power inverters eligible for section 45X and the U.S. supplier of its affiliate’s foreign-produced inverters, explains that the Commission’s proposal would nevertheless require certification of its non-covered inverters solely because they fall within the same sector. TMEIC further explains that this result would impose additional costs and delays while increasing the volume of applications that TCBs and the Commission must process. The American Clean Power Association (“ACP”) and the Secure and Advanced Non-FEOC Energy Alliance (“SAFE”) raise similar concerns about imposing certification costs and delays on non-covered domestic equipment. The National Electrical Manufacturers Association (“NEMA”) likewise opposes automatically requiring certification of every device in a Covered List sector, explaining that doing so would impose significant costs on trusted suppliers without implementing a risk identified in the underlying national-security determination.²⁶

SAFE also raises a distinct concern about an inverter that independently falls within a Covered List entry but is incorporated into a battery energy storage system or another host product. SAFE’s concern is limited to a host product containing an inverter that independently falls within the applicable Covered List entry. It therefore provides no basis for treating every inverter, or the non-covered portions of the host product, as covered equipment. Nor does it justify requiring certification throughout the inverter sector. If the Commission identifies an authorization gap involving a particular embedded-inverter configuration, any response should remain directed to the covered inverter, stay within the applicable national-security determination, and avoid imposing new requirements on unrelated, non-covered equipment.²⁷

The robotics and uncrewed aircraft systems (“UAS”) comments likewise explain why sector membership alone should not determine a device’s authorization pathway. Boston Dynamics agrees that a relatively high level of compliance verification may be appropriate, but explains that full certification of

²⁶ See *Following New National Security Determination, FCC Announces Modification of Power Inverters Entry on the Covered List*, WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233, Public Notice, DA 26-870, at 1–4 & Apps. A–B (PSHSB Aug. 20, 2026); TMEIC Comments at 8–10; ACP Comments at 9–10; NEMA Comments at 4; SAFE Comments at 5.

²⁷ See SAFE Comments at 4–5; *Third FNPRM* at 55, paras. 155–56.

every advanced robot would make little sense and supports a narrower pathway for trusted producers. Faraday Future Intelligent Electric Inc. (“Faraday”) similarly warns that sector-wide certification would impose disproportionate burdens on manufacturers and TCBs without addressing a specific security threat associated with each product. The Association for Uncrewed Vehicle Systems International (“AUVSI”) asks the Commission to preserve SDoC for specified categories of trusted UAS and to recognize comparable pathways for trusted robotics producers. Seneca likewise opposes blanket certification and asks the Commission to preserve SDoC for domestic UAS developed for public-safety uses. Although these commenters propose different mechanisms, their filings support the same conclusion: the authorization pathway should depend on the equipment and the applicable national-security determination, not a broad category label.²⁸

The Commission should reject the proposed sector-wide certification requirement and preserve SDoC and existing exemptions for equipment that does not fall within an applicable Covered List entry. Any demonstrated authorization gap should be addressed through a rule tailored to that gap. If an enumerated national-security source later issues a qualifying determination covering additional equipment, the Commission may implement that determination according to its terms.

If the Commission nevertheless proceeds with a broader certification requirement, it should preserve otherwise applicable authorization pathways for domestic equipment and for equipment receiving Conditional Approval through the applicable national-security process. The *Third FNPRM* also identifies other categories that may warrant continued access to SDoC, including U.S.-based companies relying on U.S. or allied-country suppliers. Preserving those pathways would reduce the proposal’s reach, but it would not justify requiring certification of other non-covered equipment merely because it shares a sector with covered products. Equipment outside the applicable Covered List entry should retain the authorization pathway for which it otherwise qualifies.²⁹

B. Universal SDoC Registration Would Create New Burdens Without Verifying Compliance or Enabling Marketplace Verification

INCOMPAS continues to oppose requiring every device authorized through SDoC to be registered with the Commission. SDoC is not an absence of regulation. Existing rules require the responsible party to ensure that the equipment complies with applicable technical standards, identify the product, provide specified compliance information, retain supporting records, and make those records available to the

²⁸ See Boston Dynamics Comments at 6; Faraday Comments at 4; AUVSI Comments at 1–2; Seneca Comments at 4–5.

²⁹ See *Third FNPRM* at 54, para. 154; TMEIC Comments at 9–10; ACP Comments at 9–10; SAFE Comments at 5; AUVSI Comments at 1–2.

Commission upon request. INCOMPAS, ITI, CTIA, CCIA, TMEIC, and other commenters explain that universal registration would add another filing obligation without remedying a demonstrated deficiency in those requirements.³⁰

A registration number would establish only that information was submitted; it would not provide independent evidence that the device complies. Registration would rely on representations from the same responsible party subject to the existing SDoC requirements, and a party willing to make a false SDoC representation could also submit false registration information. Indeed, the Commission previously concluded that automatic filing of SDoC information would not provide additional assurance of compliance when the required measurements and testing had been performed properly.³¹ Evolving security concerns and improved database capacity may make collection easier, but they do not demonstrate that collecting a record for every SDoC device would prevent false claims or identify covered equipment. Before imposing universal registration, the Commission must identify a demonstrated deficiency in the existing framework and explain how an additional filing would materially address that deficiency rather than merely reproduce existing information in a Commission database.

The filings supporting broader registration do not supply that missing justification. WISPA—The Association for Broadband Without Boundaries (“WISPA”) argues that an FCC database would increase confidence that listed products comply. INCOMPAS shares WISPA’s interest in reliable information for network providers selecting equipment. But an unverified database entry may create the appearance of assurance without providing the verification on which that assurance depends. WISPA does not explain how registration would detect false submissions or why equipment presenting no identified supply-chain risk should bear the same obligation. AUVSI does not oppose registration in principle but requests a realistic transition period and protection of sensitive information. Those safeguards could mitigate some consequences of registration, but they do not establish the need for a universal mandate.³²

If the Commission nevertheless proceeds and identifies a clearly defined, higher-risk subset of SDoC equipment for which an accessible compliance record would address a demonstrated risk, it should adopt the narrower approach described in INCOMPAS’s opening comments. The responsible party or manufacturer should be permitted to use the device’s existing model identifier and maintain a publicly searchable record containing only the minimum nonconfidential information necessary to identify the

³⁰ See *Third FNPRM* at 71–72, paras. 211–15; 47 CFR §§ 2.906(a)–(b), 2.938, 2.945, 2.1074(a), 2.1077; ITI Comments at 23–26; CTIA Comments at 26; CCIA Comments at 25–27; TMEIC Comments at 14–16.

³¹ See *Third FNPRM* at 71, paras. 211–13; INCOMPAS Comments at 50–52.

³² See WISPA Comments at 5; AUVSI Comments at 8.

device and locate its compliance statement. The record should exclude HBOM and SBOM information and all confidential commercial, proprietary, supply-chain, cybersecurity, and other security-sensitive information. This approach would avoid a universal FCC database and reduce the risks associated with concentrating sensitive information in a government repository, while preserving INCOMPAS's primary position that the record does not justify an SDoC registration mandate.³³

Universal registration also would not make the Commission's proposed marketplace-verification requirement workable. A registration record would show only that a responsible party submitted information concerning a model; it would not give a marketplace that never possesses or inspects the item an independent means to determine whether a particular unit offered by a third-party seller corresponds to that record. As demonstrated in the record, the problem is especially acute for used and refurbished products and for live or one-of-a-kind sales that may lack a static, item-specific listing. eBay and Whatnot explain that marketplaces cannot verify product-specific facts that neither they nor their sellers possess. AUVSI supports requiring online marketplaces to verify, rather than merely display, equipment-authorization and compliance information. Its filing, however, does not explain how a marketplace that never possesses or takes title to a device could independently confirm that seller-supplied information corresponds to the particular device offered for sale.³⁴

The Commission should not respond to those structural limitations by expanding the information required through SDoC registration or imposing manufacturer-level diligence on online marketplaces. It should instead preserve the distinctions already adopted: marketplaces need not display SDoC compliance information; listings for used devices and products offered by small third-party sellers remain exempt from the FCC ID requirement; and a marketplace that never has physical access to or takes title to a device need only validate the seller-provided FCC ID and obtain the seller's certification, rather than independently determine that the identifier corresponds to the particular device. Any additional obligation should permit reasonable reliance on information supplied by the responsible party or seller absent actual knowledge, or sufficiently specific notice, that the information is materially inaccurate. The Commission also should not require retailers or marketplaces to verify a purchaser's license before completing a sale when those intermediaries cannot reliably perform that task.³⁵

³³ See INCOMPAS Comments at 50, 53–54.

³⁴ See *Third FNPRM* at 72, paras. 214–15; AUVSI Comments at 8; eBay Comments at 6–9, 13–14; Whatnot Comments at 2–3.

³⁵ See *Third R&O* at 29–30, paras. 70–75; 47 CFR § 2.803(c).

IV. THE COMMISSION SHOULD REJECT THE FORTY-UNIT IMPORTATION LIMIT AND PRESERVE WORKABLE TESTING, EVALUATION, AND R&D PATHWAYS

INCOMPAS opposes the proposed forty-unit importation limit because the Commission has not demonstrated it would advance national security, and the record shows that it would impede legitimate testing, evaluation, and product development. The Commission proposes reducing the number of units of covered equipment that may be imported per model from 4,000 to forty for those purposes without advance written approval from the Chief of the Office of Engineering and Technology (“OET”). Its tentative conclusion that forty units “seems to be sufficient” rests on the Commission’s general “experience dealing with device testing,” rather than evidence concerning the technologies affected by the proposal. The Commission identifies no misuse of the existing testing pathway, diversion of testing units into commercial markets, or product-specific analysis showing that forty units can accommodate the development requirements of communications equipment, advanced robotics, UAS, and utility-scale power systems.³⁶

The record instead demonstrates that legitimate testing requirements vary substantially by product and program. Humanoid explains in its comments that industrial-robotics evaluations may require concurrent fleet testing, engineering spares, laboratory testing, multiple facilities, and successive hardware generations.³⁷ ITI describes testing at different development stages and across environments and configurations, including mesh-network performance and quality-assurance work requiring a statistically meaningful number of units.³⁸ Faraday and NAM likewise describe multi-site testing under varied operating conditions.³⁹ AUVSI points to field trials and pilot production runs for UAS and robotics, while ACP explains that utility-scale manufacturers may need more than forty units for engineering, reliability testing, cybersecurity analysis, and development of compliant U.S.-produced alternatives.⁴⁰ These examples refute the assumption that a single forty-unit allowance can accommodate legitimate development programs across every affected technology.

The proposed limit also is difficult to reconcile with the Commission’s existing importation rules. Those rules permit up to 400 devices for trade-show demonstration and up to 12,000 certification-subject devices for specified pre-sale activities after compliance testing and submission of the certification

³⁶ See *Third FNPRM* at 55–56, paras. 159–61 & App. B (proposing 47 CFR § 2.1204(c)(2)); 47 CFR § 2.1204(a)(3). The current rule permits importation of up to 4,000 units of a particular model for specified testing, evaluation, and product-development purposes and authorizes the OET Chief to approve a greater quantity.

³⁷ Humanoid Comments at 4–6.

³⁸ ITI Comments at 13–14.

³⁹ Faraday Comments at 5; NAM Comments at 3.

⁴⁰ AUVSI Comments at 6; ACP Comments at 12–13.

application. Yet the proposal would permit only forty units of covered equipment for engineering, security testing, and product development absent advance OET approval.⁴¹ Although the activities serve different purposes, the disparity underscores the absence of a reasoned basis for the proposed number. Engineering and security testing precede responsible product deployment, and the Commission has not explained why those activities warrant a substantially lower allowance or why enforceable controls against marketing and distribution would be inadequate for a larger testing program.⁴²

Controlled testing also advances, rather than undermines, the national-security objectives of this proceeding. U.S. companies may need access to foreign equipment to identify vulnerabilities, evaluate interoperability, understand the capabilities of foreign competitors, qualify alternative suppliers, and develop secure replacements. Importation for those limited purposes does not authorize sale or commercial deployment. The equipment remains subject to the conditions governing its entry and to the Commission's prohibition against marketing covered equipment. The Commission has not shown why the security risk changes at forty units or why appropriate controls would be insufficient for a larger, legitimate testing program.

The record does not establish a single replacement number suitable for every technology. Humanoid proposes 200 units per model and hardware generation, while Faraday recommends at least 500.⁴³ INCOMPAS does not endorse either figure as a generally applicable limit. The different proposals instead confirm that testing needs depend on the equipment, the number of facilities, and the scope of the development program. The Commission should retain a generally available threshold substantially above forty units and provide a prompt, streamlined OET process for quantities exceeding that threshold. OET should apply clear criteria and issue decisions within a period that allows manufacturers to plan and conduct legitimate testing. A discretionary process that produces unpredictable or delayed decisions would not provide a workable alternative.⁴⁴

The protected activities should expressly include software validation, AI-model testing, cybersecurity research, and controlled collection of physical-world training data. Robotics and other AI-enabled systems require iterative testing across multiple units and operating environments before

⁴¹ See 47 CFR § 2.1204(a)(4) (permitting importation of up to 400 devices for trade-show demonstration); *id.* § 2.1204(a)(11) (permitting importation of up to 12,000 devices per FCC ID for specified pre-sale activities after compliance testing has been completed and an application for certification has been submitted); *Third FNPRM* at 56, paras. 160–61 & App. B (proposing 47 CFR § 2.1204(c)(2)).

⁴² ITI Comments at 13–14; see 47 CFR § 2.1204(a)(4), (11).

⁴³ Humanoid Comments at 5–6; Faraday Comments at 5.

⁴⁴ ITI Comments at 14; AUVSI Comments at 6; ACP Comments at 13.

developers can assess safety, security, and performance. Physical hardware also may be necessary to train or validate software and AI models intended for use with lawful equipment. CCIA and ITI explain that controlled access to covered equipment can support security research and the development of compliant alternatives.⁴⁵ The Commission should preserve those activities subject to controls against unauthorized marketing or deployment.

The Commission also should preserve a limited allied-country R&D protection for equipment and components obtained through trusted allied-country supply chains and imported solely for controlled testing or product development. Such protection should supplement, not replace, the generally available importation threshold and streamlined OET process. It also must remain consistent with the applicable national-security determination. If that determination reaches the equipment, the Commission should coordinate with the enumerated source or recognize an applicable Conditional Approval. An exception under section 2.1204 would permit importation for the specified research purpose; it would not authorize the marketing, sale, or deployment of equipment that remains prohibited under other Commission rules.⁴⁶

Finally, any new restriction should apply prospectively and include predictable approval and transition procedures. Equipment lawfully imported under the existing rule should remain available for the purposes, and subject to the conditions that governed its importation. ITI and AUVSI explain that case-by-case OET review will not protect legitimate testing programs unless the agency applies clear standards and acts within a workable period. ACP similarly emphasizes the time manufacturers need to modify their development processes, while NTCA explains that uncertainty concerning the duration and terms of Conditional Approvals complicates purchasing decisions for smaller network operators. These considerations reinforce the need for a workable default threshold, prompt OET review, and prospective implementation. They do not support restricting legitimate testing and development to forty units.⁴⁷

V. THE COMMISSION SHOULD NOT APPLY A SINGLE OVERBROAD DEFINITION OF “PRODUCED IN A FOREIGN COUNTRY” ACROSS COVERED LIST SECTORS

The existing production-location-based Covered List entries do not employ a single definition of foreign production. The UAS and router entries use the phrase “produced in a foreign country,” and the Commission has issued guidance and established Conditional Approval processes concerning those entries. The later advanced-robotics determination expressly defines “foreign-produced” by reference to the federal

⁴⁵ CCIA Comments at 13–14; ITI Comments at 20–21; INCOMPAS Comments at 39–43.

⁴⁶ AUVSI Comments at 1–2; Humanoid Comments at 7, 9; see 47 U.S.C. § 1601(a), (c); 47 CFR §§ 2.803, 2.903, 2.1204; *Third FNPRM* at 55–56, 63, paras. 159–61, 184; INCOMPAS Comments at 41–43.

⁴⁷ Humanoid Comments at 6; ITI Comments at 14; AUVSI Comments at 6; ACP Comments at 13; NTCA Comments at 5–6.

“domestic end product” standard. The modified power-inverter entry uses a different formulation, excluding inverters that either are eligible for the advanced-manufacturing production credit under section 45X or qualify as domestic end products. The *Third FNPRM* nevertheless proposes a generally applicable interpretation of “produced in a foreign country” and asks whether it should govern all existing and future production-location-based entries.⁴⁸

Against that entry-specific background, the record reveals no consensus on a single definition. ITI urges the Commission to distinguish trusted foreign partners from foreign adversaries and to use an established country-of-origin framework rather than the proposed domestic-end-product test.⁴⁹ CCIA likewise rejects treating all foreign production alike and opposes using procurement or consumer-labeling standards to define Covered List treatment.⁵⁰ Boston Dynamics urges recognition of allied-country inputs and explains that the Buy American Act standard was not designed for this national-security purpose.⁵¹ Other commenters propose materially different approaches. Faraday supports harmonizing the definition with the domestic-end-product standard used in the advanced-robotics and inverter determinations.⁵² Humanoid supports a conjunctive reading of the ambiguous proposed rule text, under which a device would be foreign-produced only if it both fails the domestic-end-product test and is designed or developed abroad.⁵³ SAFE urges the Commission to incorporate the prohibited-foreign-entity safeguards associated with section 45X and to require equivalent safeguards under any domestic-end-product pathway for power inverters.⁵⁴ ACP favors a generally uniform domestic-end-product test unless the underlying determination expressly establishes a different standard for a particular equipment category.⁵⁵ These materially different proposals confirm that the record does not support automatically applying a procurement, tax, consumer-labeling, or other preexisting definition to every Covered List entry.

That disagreement matters because “produced in a foreign country” is not defined in the Secure Networks Act and does not itself supply the national-security judgment required by the statute. The phrase acquires regulatory significance through the particular national-security determination underlying a

⁴⁸ See *Third FNPRM* at 67–69, paras. 197–201; Faraday Comments at 7; SAFE Comments at 2–3; *Power Inverters Covered List Public Notice* at 1–4 & App. B.

⁴⁹ See ITI Comments at 3, 19–20.

⁵⁰ See CCIA Comments at 22–23.

⁵¹ See Boston Dynamics Comments at 5.

⁵² See Faraday Comments at 7.

⁵³ See Humanoid Comments at 8.

⁵⁴ See SAFE Comments at 2–3.

⁵⁵ ACP Comments at 4–5.

Covered List entry. The Commission therefore should begin with that determination and explain how any production test implements its text and identified risk. A definition developed for federal procurement, tax incentives, consumer labeling, or one product category could materially enlarge the scope of a different determination. INCOMPAS agrees that regulated parties need clear and administrable rules, but the Commission should provide that clarity by publishing or codifying the test applicable to each entry, consistent with the underlying determination, and obtaining clarification from the issuing source where necessary. Uniformity cannot justify rewriting or expanding the determination that the Commission is charged with implementing.⁵⁶

INCOMPAS therefore continues to favor a substantial-transformation framework tied to foreign-adversary risk as the more appropriate starting point. That framework generally asks whether processing in a country created a new and different article with a distinctive name, character, or use, including which operations imparted the finished article's essential character. It does not require every component or production input to originate in the United States. The framework also preserves the critical distinction between origin and risk: substantial transformation may identify where a finished device was produced, but the underlying national-security determination must establish why production in that location presents the unacceptable risk required by the statute. The Commission should not use a country-of-origin definition to supply a risk determination that the designated national-security source did not make. Any adopted test must therefore remain within the language and risk assessment of the determination it implements and should not presume that production in an allied or partner country presents the same risk as production involving an identified foreign adversary.⁵⁷

VI. THE COMMISSION SHOULD REJECT UNIVERSAL TERM LIMITS AND PRESERVE PROCEDURAL SAFEGUARDS

A. The Commission Should Reject Fixed Terms for Equipment Authorization

INCOMPAS continues to oppose imposing a fixed term on equipment authorizations. The *Third FNPRM* observes that equipment lifecycles vary, manufacturers may eventually discontinue software and security updates, and the Commission's rules continue to evolve. But it does not identify a demonstrated instance in which an authorization's indefinite duration caused a compliance failure or prevented the Commission from addressing a newly identified national-security risk. Nor does it explain what gap

⁵⁶ See 47 U.S.C. § 1601(a)–(d); *Third R&O* at 17, para. 36; *Third FNPRM* at 67–69, paras. 197–201; INCOMPAS Comments at 44–49.

⁵⁷ See INCOMPAS Comments at 48–49; see also ITI Comments at 3, 19–20; CCIA Comments at 22–23; Boston Dynamics Comments at 5.

automatic expiration would close that targeted action under the Commission’s existing rules cannot address. An equipment-certification grant reflects a determination, based on the application and supporting materials, that the equipment complies with the requirements applicable at the time of grant. The passage of time alone does not establish that the equipment’s design has changed, that it has become noncompliant, or that it presents a newly identified security risk. Where evidence concerning a particular authorization satisfies the grounds for revocation, withdrawal, or limitation under section 2.939 of the Commission’s rules, the Commission may address that authorization directly. Universal expiration would replace that risk-based approach with a calendar-based presumption requiring renewal or reauthorization regardless of whether anything material has changed.⁵⁸

The record documents the substantial consequences of that indiscriminate approach. Communications, enterprise, industrial, automotive, energy, and consumer equipment may remain in service for a decade or longer, often as part of larger systems that depend on continuing maintenance, compatible replacement units, spare parts, and security support. Periodic reauthorization could disrupt network and infrastructure planning, maintenance, repair, and secondary markets even where the equipment remains functional and compliant. It also could require manufacturers to repeat engineering, testing, legal, and compliance work for unchanged products while requiring laboratories, TCBs, and Commission staff to reconsider large numbers of existing authorizations. A streamlined renewal process might reduce, but would not eliminate, those burdens. The record does not demonstrate that universal periodic review would produce a security benefit that targeted review of an identified concern could not provide. Those resources would be better directed toward identified vulnerabilities, noncompliant products, and equipment presenting a substantiated national-security concern.⁵⁹

FDD’s contrary proposal does not establish a need for universal expiration. FDD suggests that a uniform expiration date would permit the Commission to periodically reconsider emerging risks. But an authorization’s age is not a proxy for risk, and periodic reconsideration is not a security measure. FDD’s brief proposal does not identify a device-specific or category-specific deficiency that automatic expiration would remedy, demonstrate that the Commission’s targeted authorities are inadequate when a particular concern arises, or address the lifecycle and administrative consequences documented throughout the record.

⁵⁸ See *Third FNPRM* at 70, paras. 208–10; 47 CFR §§ 2.907, 2.911, 2.939; INCOMPAS Comments at 63–66; ITI Comments at 21–23; CCIA Comments at 24–25; Faraday Comments at 4–5.

⁵⁹ See INCOMPAS Comments at 63–66; ITI Comments at 21–23; CTIA Comments at 24–26; TIA Comments at 35–36; CCIA Comments at 24–25; Ciena Comments at 15–16; CTA Comments at 40–41; MEMA Comments at 8–9; ACP Comments at 14–15; eBay Comments at 10–12; CEDIA Comments at 3.

The Commission should respond to evidence of an actual compliance or national-security risk, not presume that every authorization becomes suspect with age.⁶⁰

If the Commission nevertheless adopts a term limit, it should apply only to equipment covered by a qualifying Covered List determination and only to continued marketing after the term expires. Expiration should not prohibit the continued operation of equipment that was lawfully authorized and deployed, and authorizations issued before the effective date of any new rule should be grandfathered. Those limitations would mitigate, but not resolve, the absence of a demonstrated need for automatic expiration.⁶¹

B. Any Expedited Revocation Process Must Preserve Procedural Safeguards

Section 2.939 of the Commission's rules already authorizes the Commission to revoke or limit an equipment authorization on specified grounds, including false statements, technical noncompliance, unauthorized equipment changes, and subsequently discovered conditions that would have warranted denial of the original application. The current rule generally requires revocation to proceed in the same manner as revocation of a radio-station license, subject to a narrower ten-day process where an application falsely represented that equipment was not prohibited and the Commission subsequently determines that the equipment is covered.⁶²

The *Third FNPRM* proposes to remove that general procedural requirement and extend the streamlined process to cases involving willful false statements or misrepresentations, willful failure to provide required information, and termination of a Conditional Approval. It also seeks comment on using an abbreviated process for all revocations involving covered equipment. FDD similarly supports streamlined revocation for willful false statements or misrepresentations associated with a Conditional Approval. INCOMPAS recognizes that prompt action may be appropriate when an authorization rests on willful deception, a grantee willfully withholds required information, a terminated Conditional Approval removes the basis for an authorization, or a genuine emergency implicating public health, interest, or safety requires immediate action. Those circumstances do not, however, justify making an abbreviated process the default whenever an authorization involves covered equipment or a potential supply-chain concern.⁶³

⁶⁰ FDD Public Comment at 5 (recommending “a uniform automatic expiration date for all equipment authorizations” to permit reconsideration of emerging risks).

⁶¹ See INCOMPAS Comments at 65–66; ITI Comments at 22–23; Ciena Comments at 15–16; CTA Comments at 40–41; ACP Comments at 14–15.

⁶² See 47 CFR § 2.939(a)–(b), (d).

⁶³ See *Third FNPRM* at 63–64, paras. 182–86 & App. B (proposing revisions to 47 CFR § 2.939(c)–(d)); FDD Public Comment at 5; INCOMPAS Comments at 60–61; ITI Comments at 17–18; CTIA Comments at 33; TIA Comments at 30–31.

A disputed question about a device’s producer, components, production location, or eligibility for a Conditional Approval presents a materially different case. Resolving such a dispute may require technical analysis and information from multiple tiers of suppliers outside the grantee’s direct control. For disputes of that kind, ten days ordinarily will not provide a meaningful opportunity to obtain the relevant information, evaluate the Commission’s evidence, and prepare an adequate response. The Commission should provide written notice identifying the authorization at issue and the factual evidence and legal grounds supporting proposed revocation. Where material facts are contested, it should allow at least 30 days to respond and supplement the record, absent an immediate threat to public health or safety, and preserve a meaningful avenue for Commission review. An emergency timetable should not be used merely to accelerate an ordinary compliance dispute.⁶⁴

The Commission also should distinguish willful deception from an inadvertent or correctable error, incomplete third-party information, or a reasonable disagreement over the application of a Covered List entry. Except in cases of willfulness or circumstances in which public health, interest, or safety requires otherwise, section 558(c) of the Administrative Procedure Act makes withdrawal, suspension, revocation, or annulment of a license lawful only if the licensee first receives written notice of the facts or conduct at issue and an opportunity to demonstrate or achieve compliance.⁶⁵ Consistent with that principle, the Commission should permit correction, supplemental documentation, or appropriate product-specific mitigation where those measures can resolve the concern. Any final revocation decision should state its factual and legal basis, address the consequences for equipment already marketed and deployed, and provide an appropriate transition unless the Commission separately determines that continued operation presents an immediate threat.

VII. CONCLUSION

For the foregoing reasons, INCOMPAS urges the Commission to reject broadly applicable filing, registration, certification, and expiration mandates that the record has not shown to be necessary, lawful, or workable. The Commission should implement the Covered List according to the determinations made by the national-security sources Congress designated and preserve practical pathways for testing and deploying trusted equipment. That targeted approach will protect national security and strengthen supply-

⁶⁴ See *Third FNPRM* at 63–64, paras. 184–86 & App. B; 47 U.S.C. § 312(c); INCOMPAS Comments at 60–61; ITI Comments at 17–18; CCIA Comments at 19–20; ACP Comments at 13–14.

⁶⁵ See 5 U.S.C. § 558(c); 47 CFR §§ 1.106, 1.115; *Third FNPRM* at 63–64, paras. 184–86; INCOMPAS Comments at 60–61; ITI Comments at 17–18; CTIA Comments at 33; CCIA Comments at 19–20; ACP Comments at 13–14.

chain security while allowing INCOMPAS members to continue investing in the communications networks, cloud facilities, and data centers essential to American AI and advanced technologies leadership.

Respectfully Submitted

/s/ *Staci L. Pies*

Staci L. Pies
Senior Vice President,
Government Relations and Policy
INCOMPAS
1100 G Street, N.W., Suite 800
Washington, DC 20005
spies@incompas.org
202-872-5745

September 28, 2026