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

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

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 8, 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INCOMPAS members build and operate the communications networks, cloud facilities, and data centers that provide the physical foundation for American leadership in artificial intelligence. High-capacity fiber connects computing facilities and carries the enormous volumes of data required to develop and deploy advanced AI services. Data centers provide the computing and storage capacity those services depend on. These investments support skilled construction and technical employment while expanding the digital capacity available to businesses throughout the economy. Delays in obtaining necessary equipment, uncertainty about lawful suppliers, or unnecessary duplication in equipment-authorization procedures can therefore affect far more than an individual device. They can increase deployment costs, slow infrastructure construction, and make it more difficult for American companies to compete at the pace required by the global AI race.

The Administration's commitment to American AI leadership is unequivocal. Executive Order 14179 establishes a national policy to sustain and enhance American AI leadership to promote economic competitiveness and national security. America's AI Action Plan makes building American AI infrastructure a central element of that policy and calls for rapid data-center development. Executive Order 14318 likewise identifies AI data centers and the infrastructure that powers them as important to national security and economic prosperity. More recently, the Administration emphasized that advanced AI capabilities strengthen the Nation and that government should work with industry to deploy secure technology rapidly.[1] These policies

[1] Exec. Order No. 14,179, § 2, 90 Fed. Reg. 8741, 8741 (Jan. 23, 2025); White House, *Winning the AI Race: America's AI Action Plan*, at 1, 5 (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf; Exec. Order No. 14,318, § 1, 90 Fed. Reg. 35385, 35385 (July 23, 2025); Exec. Order No. 14,409, § 1, 91 Fed. Reg. 34565, 34565 (June 2, 2026).

recognize that security and infrastructure deployment must reinforce one another. A regulatory approach that unnecessarily delays access to trusted equipment or discourages investment could undermine the leadership that the Administration seeks to preserve.

INCOMPAS shares the Commission's commitment to national security and secure communications supply chains. Its members have a direct interest in preventing equipment that presents an identified national-security risk from entering American networks. They also must be able to obtain, integrate, update, and maintain equipment throughout its useful life. Their experience demonstrates why supply-chain regulation must focus on identifiable risks and account for the information and control available to the party expected to comply. Modern communications and computing equipment is developed through complex supply chains extending across multiple tiers. Broad or ambiguous rules can exclude trusted products, expose applicants to liability for information they cannot independently verify, and divert resources away from infrastructure deployment without materially improving security.

Congress established a defined process for addressing unacceptable supply-chain risks. The Secure Networks Act assigns specified national-security sources responsibility for making the determinations that support Covered List entries. The Commission has acknowledged that it cannot add equipment or services to the Covered List on its own initiative. The Secure Equipment Act then directs the Commission not to review or approve equipment-authorization applications involving equipment on that list.[2] The Commission has an important implementation

[2] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, § 2, 133 Stat. 158, 158–60 (2020) (codified as amended at 47 U.S.C. § 1601); Secure Equipment Act of 2021, Pub. L. No. 117-55, § 2(a)(2), 135 Stat. 423, 423–24 (2021) (codified at 47 U.S.C. § 1601 note); *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 (July 23, 2026) (*Third R&O* and *Third FNPRM* as appropriate), corrected by Erratum, DOC-424161A1 (OET Aug. 13, 2026).

role, but an implementing definition should not materially expand the equipment, components, or entities reached by the underlying national security determination. The D.C. Circuit's decision in *Hikvision USA, Inc. v. FCC* reinforces the need to keep the Commission's implementing definitions reasonably tied to the statutory language incorporated into the Covered List.[3]

The Communications Act does not supply an alternative source of unlimited supply-chain authority. Section 302(a) authorizes reasonable regulations governing the interference potential of devices capable of emitting radiofrequency energy and certain standards addressing susceptibility to radiofrequency interference. That authority supports rules governing software when software controls a transmitter's compliance with authorized radiofrequency parameters. It does not, without more, transform the equipment-authorization program into a general system for regulating the provenance of every component incorporated into a device. Sections 4(i) and 303(r) likewise do not independently enlarge the Commission's jurisdiction; an exercise of ancillary authority must remain connected to a responsibility that Congress assigned to the Commission.[4]

These statutory boundaries are particularly important where the *Third FNPRM* contemplates treating equipment as prohibited because it contains software, firmware, or another component not encompassed by the applicable Covered List determination. They also bear directly on proposals that would require comprehensive Hardware Bill of Materials ("HBOM") and Software Bill of Materials ("SBOM") submissions from applicants with no demonstrated connection to covered equipment. The Commission should distinguish targeted information

[3] *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948–50 (D.C. Cir. 2024).

[4] 47 U.S.C. §§ 154(i), 302a(a), 303(r); *American Library Ass'n v. FCC*, 406 F.3d 689, 691–92, 698–708 (D.C. Cir. 2005); *Comcast Corp. v. FCC*, 600 F.3d 642, 654–61 (D.C. Cir. 2010).

needed to implement a particular national-security determination from a universal supply-chain reporting system. The latter would impose substantial compliance burdens and concentrate highly sensitive information in a repository that itself could become a security target.

The same discipline should guide the Commission's consideration of proposed changes to established authorization and enforcement processes. Obligations should rest with parties that possess the information and authority necessary to comply. A manufacturer or responsible party generally controls product design, testing records, and the applicable compliance documentation; a marketplace that never possesses the device ordinarily does not. An abbreviated revocation process likewise should not displace adequate notice and meaningful review where the facts are disputed. These procedural protections do not diminish national security. They improve the reliability of Commission decisions and reduce the risk that lawful equipment will be removed or delayed because of incomplete information.

INCOMPAS's alternative recommendations should not be understood as endorsing the broader mandates proposed in the *Third FNPRM.* They identify necessary safeguards if the Commission proceeds despite INCOMPAS's primary objections. Any narrower rule would need to correspond to an evidence-based risk and reflect the regulated party's actual access to the relevant information. It would also need enforceable confidentiality protections and a workable transition. Preserving those alternatives allows INCOMPAS and its members to engage constructively as the record develops without conceding that the Commission has demonstrated either the need or the statutory basis for the proposals in their present form.

American technological leadership and national security are mutually reinforcing. The most durable supply-chain protections will be those that rest on Congress's allocation of responsibility, respond to demonstrated threats, and preserve the ability of American companies

to build the infrastructure on which the Nation's economic and security interests increasingly depend.

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

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

COMMENTS OF INCOMPAS

INCOMPAS hereby submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") Third Further Notice of Proposed Rulemaking ("*Third FNRPM*") examining additional steps to strengthen the Commission's equipment authorization program against national security risks to the communications supply chain.[5]

I. INTRODUCTION

INCOMPAS appreciates the Commission's continued efforts to implement the Covered List[6] and secure U.S. communications networks pursuant to its statutory obligations under the Secure Networks Act ("SNA") and Secure Equipment Act ("SEA").[7]

---

[5] *Third FNPRM*.

[6] See FCC, List of Equipment and Services Covered By Section 2 of The Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist (last updated Aug. 20, 2026) ("FCC Covered List").

[7] 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. §§ 1601–09) ("Secure Networks Act"); Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 note) ("Secure Equipment Act").

INCOMPAS shares the Commission's commitment to ensuring that devices introduced into the U.S. marketplace are secure and appropriately vetted. Several proposals in the *Third FNPRM*, however, would materially expand the equipment-authorization program beyond its traditional radiofrequency-compliance function and toward a broader supply-chain regulatory regime. Before imposing those obligations, the Commission should identify the statutory authority for each requirement and explain how the requirement would address a national-security concern within the Commission's lawful responsibilities.

Under the Secure Networks Act, the designated national-security sources—not the Commission acting on its own—must make the determinations supporting additions to the Covered List.[8] Section 302(a) of the Communications Act authorizes the Commission to adopt reasonable regulations governing the interference potential of devices capable of emitting radiofrequency energy. It also authorizes certain minimum performance standards intended to reduce the susceptibility of home electronic equipment to radiofrequency interference.[9] The Secure Equipment Act directs the Commission not to review or approve applications for equipment on the Covered List, but it does not, by its terms, provide freestanding authority over the broader supply chain for equipment that is not itself covered.[10] The Commission should therefore ensure that each new obligation is closely connected to the relevant Covered List

[8] See 47 U.S.C. § 1601(a), (c); *Third R&O* para. 36 ("The Commission lacks the authority to add to the Covered List on its own initiative.").

[9] See 47 U.S.C. § 302a(a); *Third R&O* paras. 29–31 (explaining the relationship between section 302(a), the Commission's interference authority, and the scope of the adopted logic-bearing-hardware rule).

[10] See Secure Equipment Act of 2021 § 2(a)(2), Pub. L. No. 117-55, 135 Stat. 423, 423–24 (codified at 47 U.S.C. § 1601 note); see also *Third R&O* para. 18 (describing the adopted component rule as "generally consistent" with the Secure Networks Act and Secure Equipment Act), para. 244 (identifying the statutory provisions on which the Commission relies).

determination and the risk identified by that determination. It should also explain how the obligation falls within a function Congress authorized the Commission to perform.

Proposals that do not observe these statutory guardrails could disrupt trusted supply chains without delivering a commensurate national-security benefit. They could also weaken U.S. competitiveness by delaying access to equipment needed for advanced communications and computing infrastructure. The Commission compounds that uncertainty by keeping proposals open that it previously declined to adopt because the record did not adequately support those proposals. Because product development and infrastructure planning occur years before deployment, clear and reasonably stable regulatory expectations are essential.

As members of the Administration have recognized before, "economic security is national security,"[11] and while the Commission should take action against untrustworthy gear, it must also be circumspect and pragmatic when considering sweeping proposals in this *Third FNPRM* that could sacrifice U.S. competition in the global device market without appropriate countervailing national security benefit.

INCOMPAS members build and operate the networks and data centers that enable U.S. leadership in artificial intelligence. They purchase and integrate the equipment at issue in this proceeding and must continue maintaining that equipment throughout its useful life. Rules that delay product availability or access to trusted suppliers can slow infrastructure deployment. Restrictions that impede prompt security updates can increase rather than reduce risk.

[11] Remarks by Treasury Secretary Scott Bessent before the 2026 Reagan National Economic Forum (May 29, 2026), *available at* https://home.treasury.gov/news/press-releases/sb0514.

The Commission should give substantial weight to documented operational evidence from companies that design and manufacture affected equipment, as well as from those that deploy it at scale. That evidence is necessary to determine whether a proposed restriction can be implemented within the contemplated timeframe and whether compliant alternatives exist in the required quantities. This operational evidence also allows the Commission to compare the practical burden of a proposal with its likely security benefit.

Accordingly, to ensure that the Commission's national-security efforts reinforce rather than impede U.S. technological leadership, INCOMPAS encourages the Commission to:

1. Confirm that it will not adopt the pending proposal to prohibit authorization of equipment containing components produced by an entity that is not on the Covered List solely because that entity has a foreign-adversary nexus. The Commission should close the existing record without foreclosing a focused supplemental notice if materially different evidence later warrants reconsideration.

2. Decline to prohibit equipment authorization based on the presence of, or integration with, software or firmware unless an enumerated national-security source has specifically determined that the relevant software, firmware, or integrating equipment presents an unacceptable national-security risk. The Commission should close the record on the pending proposals, including a general prohibition on downloading software, while retaining the ability to implement a future determination through a focused proceeding.

3. Decline both the proposed categorical prohibition covering all components produced by a Covered List entity and the proposed rebuttable presumption. Any

component-level authorization prohibition should remain confined to logic-bearing components or components with a distinct nexus to the provision of radiofrequency communications.

4. Reject the proposed universal Hardware Bill of Materials ("HBOM") and Software Bill of Materials ("SBOM") filing mandate and blanket certification requirements for all devices within Covered List sectors. If the Commission nevertheless proceeds, it should limit any requirement to a clearly defined, higher-risk subset supported by an evidence-based assessment. Any HBOM or SBOM disclosure should be limited to critical or RF-relevant components. The Commission should not require applicants to file HBOM or SBOM information if it cannot provide legally enforceable assurance that the information will remain nonpublic. Any expansion of mandatory certification should rest on a sector-specific record demonstrating that heightened review is reasonably connected to an identified national-security risk.

5. Preserve workable importation, testing, evaluation, and research-and-development pathways so that U.S. companies can validate interoperable and AI-enabled systems without unnecessary authorization delays. Any allied-country protection should supplement, rather than replace, a generally available streamlined Office of Engineering and Technology process and a workable numerical threshold.

6. Reject universal Supplier's Declaration of Conformity ("SDoC") registration and new requirements that would make retailers or online marketplaces independently verify SDoC compliance information when they lack physical access to or title to the equipment. If the Commission nevertheless adopts limited requirements, it

should confine registration to a clearly defined, evidence-based higher-risk subset and permit manufacturer-hosted records using existing product identifiers. Any marketplace obligation should reflect the information the marketplace controls and include reasonable-reliance and safe-harbor protections. Any expanded revocation procedure must preserve adequate notice, an opportunity to cure, and meaningful hearing and review rights.

II. THE COMMISSION SHOULD CONFIRM THAT IT WILL NOT ADOPT BROADLY SCOPED FOREIGN ADVERSARY PROHIBITIONS

A. The Third R&O Correctly Declined to Adopt the Foreign-Adversary-Nexus Proposal

The *Second FNPRM* sought comment on whether the Commission should prohibit authorization of equipment containing logic-bearing hardware components produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, even if the entity was not identified on the Covered List.[12] The *Third R&O* correctly declined to adopt that proposal. The Commission found "minimal record evidence in support of such action" and recognized that commenters had demonstrated the proposal's "enormous practical challenges."[13] Although the Commission stated that it would keep the record open, its findings support bringing the proposal to a close.

INCOMPAS agrees with the Commission's decision. A workable supply-chain rule must begin with an identifiable universe of entities and equipment. The foreign-adversary-nexus proposal instead would require an equipment-authorization applicant to determine whether an

---

[12] See *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, ET Docket No. 21-232, Second Report and Order and Second Further Notice of Proposed Rulemaking, 40 FCC Rcd 8430, 8459, para. 64 (2025) (S*econd R&O* and *Second FNPRM* as appropriate); *Third R&O* para. 15 & n.39.

[13] *Third R&O* para. 35.

entity anywhere in its supply chain is owned or controlled by a foreign adversary or subject to that adversary's jurisdiction or direction. Information necessary to make that determination may not be public or reasonably available, particularly where a component passes through multiple supplier tiers before being incorporated into the finished device.[14]

The resulting uncertainty would not yield a reliable security screen. Instead, it would expose applicants to potential liability stemming from corporate relationships they cannot independently verify. It could also exclude equipment containing components that pose no demonstrated security risk.

B. The Record and Governing Statutes Do Not Support the Commission's Proposals in this Proceeding

Congress established a specific process for identifying equipment and services that pose an unacceptable national security risk. Section 2(b) of the Secure Networks Act directs the Commission to place equipment or services on the Covered List "if and only if" the statutory criteria are satisfied. That determination must be based exclusively on one or more of the determinations identified in section 2(c). The Commission accordingly acknowledged in the *Third R&O* that it "lacks the authority to add to the Covered List on its own initiative." A rule that subjects components produced by an unlisted entity to the same authorization prohibition that applies to equipment produced by a Covered List entity would create a de facto covered class outside that statutory process. The relevant national-security agency would not have determined that the entity's equipment poses an unacceptable risk. Nor would the Commission

[14] See *Third R&O* para. 35 & n.96; Comments of the Commercial Drone Alliance, ET Docket No. 21-232, at 2–3 (filed Jan. 5, 2026) (CDA Comments); Comments of CTIA at 8–12 (CTIA Comments); Comments of NCTA – The Internet & Television Association at 4–5 (NCTA Comments); Comments of Garmin International, Inc. at 4–9 (Garmin Comments).

be implementing a Covered List entry that identifies the entity. Instead, the prohibition would arise from a generalized affiliation standard administered by the Commission.

The Secure Equipment Act does not eliminate that concern. The Act requires the Commission to stop reviewing or approving applications for equipment that is on the Covered List. It does not by its terms prohibit authorization of a device based solely on the involvement of an entity that has never been identified through the Secure Networks Act process.[15]

Section 302(a) of the Communications Act also does not provide an unlimited source of supply-chain authority. That provision authorizes reasonable regulations governing the interference potential of devices capable of emitting radiofrequency energy and certain standards intended to reduce susceptibility to interference.[16] The Commission itself relied on this statutory boundary when it confined the adopted component rule to logic-bearing hardware operating within the scope of its radiofrequency authority.[17]

Section 4(i) permits the Commission to take actions necessary to carry out functions assigned elsewhere in the Communications Act. It does not independently enlarge the Commission's jurisdiction. The D.C. Circuit has therefore required the Commission to show that an exercise of ancillary authority is reasonably ancillary to the effective performance of a responsibility Congress actually assigned it.[18] At a minimum, the Commission would need to identify that responsibility and demonstrate the required connection before imposing a

---

[15] Secure Equipment Act of 2021 § 2(a)(2), Pub. L. No. 117-55, 135 Stat. 423, 423–24 (codified at 47 U.S.C. § 1601 note).

[16] 47 U.S.C. § 302a(a).

[17] See *Third R&O* paras. 29–31 & nn.79, 82.

[18] See 47 U.S.C. § 154(i); *Am. Library Ass'n v. FCC*, 406 F.3d 689, 691–92 (D.C. Cir. 2005); *Comcast Corp. v. FCC*, 600 F.3d 642, 654–61 (D.C. Cir. 2010).

prohibition based on a foreign-adversary relationship that has not resulted in a Covered List determination.

These limits do not prevent the government from addressing a genuine threat. If an enumerated national-security source determines that equipment produced by a particular entity poses an unacceptable risk, the Secure Networks Act provides a direct mechanism to add that equipment to the Covered List.

That process gives the Commission a clear, administrable basis for implementation. It also avoids requiring individual applicants to make national-security judgments based on incomplete supplier information.

C. The Commission Should Close the Record on This Rejected Proposal

Leaving the foreign-adversary-nexus proposal unresolved indefinitely creates real regulatory consequences. Equipment manufacturers select and qualify components long before submitting a product for authorization. Replacing a component late in the development process may require redesign, additional testing, or changes to planned deployment schedules. Companies building communications networks and data centers depend on predictable access to equipment when planning infrastructure investments.

The Commission's own findings favor closing the record. Only one commenter supported the broader foreign-adversary approach, while the Commission cited substantial opposition from parties with direct experience designing and deploying affected equipment.[19] The relevant point is that the record did not establish a workable need for the proposal, and the Commission expressly recognized the substantial implementation problems it would create.

[19] See *Third R&O* para. 35 & nn.95–96.

The foreign-adversary-nexus proposal remains unresolved from the *Second FNPRM,* and the *Third FNPRM* neither renews the proposal nor seeks additional comment on its terms.[20] The Commission therefore should close the record and confirm that it will not adopt the proposal based on the existing record. If materially different evidence later warrants reconsideration, the Commission can issue a focused supplemental notice that defines the contemplated restriction and explains its legal basis. That process would allow affected parties to address current threat information and the practical consequences of the particular rule under consideration while providing the notice and opportunity for comment required by the Administrative Procedure Act.[21]

D. Any Future Foreign-Adversary-Nexus Proposal Would Require a Multi-Year Transition

If, after developing a new record through a focused further notice, the Commission adopts a foreign-adversary-nexus restriction, it should provide a multi-year implementation period that reflects equipment-development timelines and supply-chain realities.

Equipment supply chains are often multi-tiered. A manufacturer may know its direct supplier but lack visibility into the ownership or control of entities several tiers removed from the finished device. If a newly prohibited component is identified, the manufacturer may need to locate and qualify an alternative supplier. A change affecting the device's performance may also require redesign, additional testing, and further equipment-authorization work.

These steps cannot reliably be completed within a matter of months. Any future restriction should apply prospectively and only after the Commission has issued final,

---

[20] See *Third R&O* para. 35; compare *Second R&O* and *Second FNPRM* para. 64, with *Third FNPRM* paras. 128–234.

[21] See 5 U.S.C. § 553(b)–(c).

administrable criteria. Previously authorized equipment should remain authorized, and the transition period should begin only after applicants have the guidance necessary to identify the affected entities and components.

A multi-year implementation period would allow manufacturers to obtain necessary supplier information and identify compliant alternatives without unnecessarily disrupting the availability of equipment used in communications networks and data centers. It would also give the Commission time to resolve recurring interpretive questions before applicants must certify compliance.

III. THE COMMISSION SHOULD DECLINE TO EXPAND EQUIPMENT-AUTHORIZATION PROHIBITIONS TO SOFTWARE OR FIRMWARE ABSENT A SPECIFIC NATIONAL SECURITY DETERMINATION

The Commission correctly declined in the *Third R&O* to prohibit equipment authorization based on software or firmware components produced by entities identified on the Covered List. The Commission found insufficient record support for such a prohibition and recognized the attendant enforcement and oversight difficulties.[22] The *Third FNPRM* nevertheless reopens the issue by asking whether the Commission should prohibit authorization of any device "that has been integrated with the software or firmware that was produced or provided by a Covered List entity." It also asks whether the Commission should prohibit downloading such software onto communications equipment.[23]

INCOMPAS recognizes that software and firmware can create serious national-security vulnerabilities. That potential risk, however, does not itself establish the Commission's authority

[22] *Third R&O* para. 30 ("We also decline to adopt a prohibition on software or firmware components produced by entities identified on the Covered List, given the lack of support in the record and the challenges with enforcement and oversight.").

[23] *Third FNPRM* paras.150–52.

to impose a categorical prohibition or determine its proper scope. As discussed above, the Secure Networks Act requires the Covered List to rest on determinations made by the sources that Congress enumerated. The Secure Equipment Act, in turn, directs the Commission not to review or approve equipment-authorization applications for equipment that is on that list. Neither statute authorizes the Commission to treat a host device as covered merely because it contains software or firmware produced by an entity identified on the Covered List when the underlying national-security determination does not encompass that software, firmware, or integrated device. Congress also separately prohibited the use of certain FCC-administered federal subsidies to obtain or maintain covered equipment and services. That targeted funding restriction does not create a general prohibition against acquiring or downloading covered software.[24]

The Commission's treatment of Kaspersky software illustrates the proper operation of this statutory framework. The Department of Commerce conducted a review under Executive Order 13873 and made a specific determination that expressly encompassed Kaspersky cybersecurity and antivirus software integrated into third-party hardware or software. The Commission then updated the Covered List to include the identified software and subsequently confirmed that equipment integrating that software could not receive equipment authorization. The Commission did not infer a general power to prohibit software based only on the identity of its producer. It implemented an enumerated source's determination that specifically addressed the software and its integration into other products.[25]

---

[24] See 47 U.S.C. §§ 1601(b)–(d), 1602(a)(1); Secure Equipment Act of 2021, Pub. L. No. 117-55, § 2(a)(2), 135 Stat. 423, 423–24; T*hird R&O* para. 36. See also *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986) ("[A]n agency literally has no power to act . . . unless and until Congress confers power upon it."); *American Library Ass'n v. FCC*, 406 F.3d 689, 691–92 (D.C. Cir. 2005); *Comcast Corp. v. FCC*, 600 F.3d 642, 654–61 (D.C. Cir. 2010).

[25] See Department of Commerce, *Final Determination*, Case No. ICTS-2021-002, *Kaspersky Lab, Inc*., 89 Fed. Reg. 52434, 52434, 52437 (June 24, 2024); *Public Safety and Homeland Security Bureau Announces Update to List of*

The Commission's existing authority over software that controls radiofrequency operations does not bridge this statutory gap. Section 302(a) of the Communications Act authorizes reasonable regulations governing the interference potential of devices capable of emitting radiofrequency energy. Consistent with that authority, section 15.407(i) requires U-NII devices to protect against unauthorized software modifications that could cause a transmitter to operate outside its certified parameters. Section 2.944 similarly governs software loaded into software-defined radios and focuses on changes affecting frequency, output power, modulation, or other approved radiofrequency parameters. Those provisions support software-related requirements that remain tied to RF emissions and the integrity of an equipment authorization. They do not establish freestanding authority to prohibit software solely because of its source or provider, without regard to its effect on RF operations or the scope of an underlying national-security determination. Nor can section 4(i) independently supply authority untethered to a responsibility Congress delegated to the Commission.[26]

A categorical prohibition would also be exceptionally difficult to define and administer. Software incorporated into communications, network, and data-center equipment may include code developed by the device manufacturer, third-party libraries, open-source components, inherited code, and dependencies obtained through multiple tiers of suppliers. Software and firmware also change throughout a product's useful life as manufacturers correct vulnerabilities, maintain interoperability, and respond to emerging threats. The terms "produced" and

---

Covered Equipment and Services Pursuant to Section 2 of the Secure Networks Act, WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233, Public Notice, DA 24-712 (July 23, 2024); *Office of Engineering and Technology and Public Safety and Homeland Security Bureau Announce Prohibition on Authorization of Equipment that Includes Kaspersky Cybersecurity or Anti-Virus Software*, WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233, Public Notice, DA 24-886 (Sept. 3, 2024).

[26] See 47 U.S.C. §§ 154(i), 302a(a); 47 CFR §§ 2.944(a)–(c), 15.407(i); *Third FNPRM* para. 151; American Library Ass'n, 406 F.3d at 691–92; Comcast, 600 F.3d at 654–61.

"provided" do not explain whether a restriction would reach an open-source contribution, legacy code acquired from another company, a remotely managed application, or a later security update. Equipment manufacturers and operators may have no reasonable means of identifying the original source of every contribution to a complex software package or verifying whether an upstream contributor has subsequently become affiliated with an entity identified on the Covered List.

The proposed download restrictions present an additional jurisdictional and operational problem because they are not limited to the Commission's review of an equipment-authorization application. They appear to reach post-sale conduct by network operators, equipment users, and potentially other parties that may not be the applicant, grantee, or responsible party for the underlying equipment authorization. The *Third FNPRM* does not identify which party would bear responsibility for a prohibited download, whether knowledge would be required, or how the Commission would monitor compliance. The omission is particularly consequential because the Commission elsewhere recognizes that software and firmware updates can mitigate harm to consumers and proposes to preserve security patches and other necessary updates for already-authorized covered equipment. A source-based download prohibition that prevents installation of a vulnerability patch could leave deployed communications equipment less secure.

These concerns reinforce the need for the Commission to coordinate with the federal entities charged with evaluating cybersecurity and information-and-communications-technology risks. The Cybersecurity and Infrastructure Security Agency ("CISA") leads federal cybersecurity and critical-infrastructure-security programs, while the Department of Commerce evaluates covered Information and Communications Technologies ("ICTs") transactions involving foreign adversaries under Executive Order 13873 and its implementing regulations.

The Commission can give effect to a qualifying national-security determination through its equipment-authorization rules when the determination and governing statutes support that action. It should not replace the risk-specific analysis of those expert agencies with a generic rule based solely on a software developer's or provider's appearance on the Covered List.[27]

Accordingly, the Commission should decline to adopt a prohibition on equipment authorization based on software or firmware unless an enumerated source has specifically determined that the software, firmware, or equipment integrating it poses an unacceptable national-security risk. The Commission should likewise decline to adopt a general prohibition on downloading software and should close the record on these proposals. If an enumerated source later issues a determination addressing a defined category of software or firmware, the Commission can consider implementing that determination through a focused proceeding that provides adequate notice and develops a record concerning scope, compliance, and implementation.

IV. THE COMMISSION SHOULD NOT EXTEND THE AUTHORIZATION PROHIBITION BEYOND LOGIC-BEARING COMPONENTS OR COMPONENTS WITH A DISTINCT NEXUS TO THE PROVISION OF RF COMMUNICATIONS

The *Third R&O* limited its expanded authorization prohibition to devices containing logic-bearing hardware components produced by a Covered List entity, where the device would be prohibited if that entity had produced the device itself. The Commission grounded that limitation in the greater security risks presented by components capable of executing instructions, processing data, accepting firmware, or responding to remote signals. It also distinguished mechanical and other passive components that lack those capabilities. The *Third*

[27] See *Third FNPRM* paras. 152, 187–92; 6 U.S.C. § 652(c)(1)–(2); 15 CFR §§ 791.1, 791.103(c), 791.109.

Further Notice nevertheless proposes to extend the prohibition to devices incorporating any component produced by a Covered List entity, including non-logic-bearing components such as screws or nails, and separately asks whether to adopt a rebuttable presumption against authorizing such devices.

INCOMPAS supports a functional, risk-based limitation on any component-level authorization prohibition. Such a prohibition should be confined to logic-bearing components or components with a distinct nexus to the provision of RF communications. This formulation identifies the appropriate functional boundary for purposes of the proposals presented here; it should not be understood as endorsing every element or potential application of the Commission's definition of "logic-bearing hardware component" in section 2.902.[28]

An all-components rule would extend beyond the national-security determinations that Congress made the necessary predicate for the Covered List. Under the Secure Networks Act, communications equipment or a communications service may be placed on the Covered List only when an enumerated national-security source has determined that the equipment or service presents an unacceptable risk and the statutory conditions are otherwise satisfied. The Secure Equipment Act, in turn, directs the Commission not to review or approve an equipment-authorization application for equipment on that list. A determination addressing particular communications equipment produced by a Covered List entity does not, without more, establish that every component produced by that entity, or every host device incorporating one of those components, presents the same risk. Treating an entity's Covered List status as an automatic

[28] *Third R&O* paras. 16, 23–30; *Third FNPRM* paras.147–49; *id.* App. A (adding 47 CFR § 2.902).

prohibition on any device containing any item produced by that entity would sever the authorization prohibition from the determination Congress required.[29]

The Commission's authority under the Communications Act does not eliminate that statutory limitation. Section 302(a) authorizes the Commission to regulate the interference potential of devices capable of emitting radiofrequency energy in a degree sufficient to cause harmful interference. Consistent with that authority, the *Third R&O* tied its definition of a logic-bearing hardware component to the 9 kHz threshold associated with the Commission's regulation of spectrum and to the use of digital techniques or RF energy for data-processing functions. That reasoning does not establish that the Commission may disqualify an otherwise compliant device solely because a mechanical fastener or another passive component that lacks both logic-bearing capability and a distinct nexus to the provision of RF communications was produced by a Covered List entity. The Communications Act's general public-interest provisions and section 4(i) cannot independently convert the equipment-authorization program into a general supply-chain regulatory regime untethered to responsibilities assigned to the Commission by Congress.[30]

The D.C. Circuit's decision in *Hikvision USA, Inc. v. FCC* reinforces the need to maintain a meaningful statutory nexus. Although the court upheld the Commission's authority to implement the Secure Equipment Act, it vacated the Commission's definition of "critical infrastructure" because that definition was unjustifiably broad and did not adequately comport with the incorporated statutory language. An all-components rule would raise a similar concern by extending a determination concerning specified communications equipment to passive or

[29] 47 U.S.C. § 1601(b)–(d); *Secure Equipment Act* § 2(a)(2), 135 Stat. at 423–24; *Third FNPRM* para. 148.

[30] 47 U.S.C. §§ 151, 154(i), 302a(a), 303(e), (g), (r); Third R&O paras. 19, 28–29, 31; *American Library Ass'n*, 406 F.3d at 698–708; *Comcast*, 600 F.3d at 654–61; see also *Louisiana Public Service Commission*, 476 U.S. at 374.

mechanical inputs without showing that those inputs fall within the relevant determination or materially contribute to the identified risk.[31]

Nor would an all-components rule be simple in practice merely because it states a categorical standard. Its apparent simplicity would shift substantial complexity to applicants, who would have to identify the producer of every part and monitor changes throughout multilayered supply chains. Complex information technology hardware may contain thousands of components sourced from hundreds of suppliers. Many passive components are acquired through distributors, are treated as functionally interchangeable, or may be substituted during production without altering the device's performance or security posture. Requiring an applicant to establish the provenance of every connector, cable, fan, enclosure, fastener, and similar item would impose substantial investigation and recordkeeping costs without focusing those resources on components presenting the functions relevant to the asserted security risk.

Those burdens would directly affect the infrastructure required for U.S. leadership in artificial intelligence. If a manufacturer discovered late in a product-development cycle that an otherwise interchangeable passive component came from a Covered List entity, an all-components prohibition could require qualification of an alternative supplier or redesign of the product. That process could delay the introduction of servers and other advanced computing and networking infrastructure even though the component at issue could not execute code, access data, respond to remote instructions, or otherwise affect the provision of RF communications. The resulting disruption would not be proportionate to the security benefit of the proposed restriction.

[31] *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948–50 (D.C. Cir. 2024)*; Third R&O* paras. 6, 20.

INCOMPAS recognizes that concentrated reliance on foreign suppliers can create legitimate resilience concerns. But concern about dependence on strategically important inputs does not establish that every component presents an unacceptable national-security risk. Indeed, the National Security Strategy language cited by the Commission addresses dependence on "core components," not every physical input incorporated into a device. Passive components can affect product reliability, but components lacking programmable functionality or a distinct RF nexus ordinarily do not present the hidden-instruction, remote-activation, or data-access risks on which the Commission relied when adopting its logic-bearing-hardware rule. The record therefore does not support treating every component produced by a Covered List entity as presenting an equivalent security risk.[32]

The proposed rebuttable presumption would not cure these defects. It would still treat every component produced by a Covered List entity as disqualifying unless the applicant proved that the resulting device does not present an unacceptable risk. Applicants first would have to identify and trace every component and then develop evidence addressing its function and risk, even when the component is a screw or another passive part. A clear-and-convincing-evidence standard would make that burden especially severe, but a preponderance standard would not correct the threshold problem: either approach would shift the burden to applicants without a predicate determination identifying the component or resulting device as presenting an unacceptable risk. The Commission therefore should decline to adopt the proposed presumption.

[32] *Third R&O* paras. 24–29, 31–35; *Third FNPRM* para. 148 & nn.280–83; CDA Comments at 2–3; CTIA Comments at 8–12; NCTA Comments at 4–5; Garmin Comments at 4–8.

If it nevertheless adopts a presumption, its scope should not extend beyond logic-bearing components or components with a distinct nexus to the provision of RF communications.[33]

Federal coordination is warranted, but the Commission must accurately describe the existing federal regimes. The Commerce Department's Entity List principally imposes restrictions on exports, reexports, and in-country transfers involving listed parties; it does not create a safe harbor governing the importation or authorization of end products containing components. Commerce's Information and Communications Technology and Services ("ICTS") program separately provides a threat-based process for reviewing ICTS transactions subject to U.S. jurisdiction and imposing appropriate mitigation or prohibitions. Before adding another component-level restriction, the Commission should coordinate with Commerce, identify the regulatory gap the FCC proposal is intended to address, and avoid imposing inconsistent provenance requirements. Compliance with one federal regime may not automatically establish compliance with another, but that is a reason for coordinated and risk-specific regulation, not for an overlapping all-components prohibition.[34]

The Commission therefore should decline both the categorical all-components proposal and a presumption reaching the same indiscriminate universe of components. Any component-level authorization prohibition should remain confined to logic-bearing components or components with a distinct nexus to the provision of RF communications. That functional limitation would permit the Commission to address the risks identified in the record without

---

[33] *Third FNPRM* para. 149; 47 U.S.C. § 1601(b)–(d).

[34] Exec. Order No. 13,873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (May 17, 2019); 15 CFR §§ 791.1, 791.103(c), 791.109; 15 CFR § 744.11 & supp. no. 4 to pt. 744.

converting equipment authorization into a requirement to trace and evaluate every passive or mechanical input incorporated into a device.

V. THE COMMISSION SHOULD REJECT THE "ANY MAJOR STAGE" DEFINITION OF "PRODUCED BY" AND FOCUS ON EXCLUSIVE OR PRIMARY ONGOING CONTROL

The Commission seeks comment on whether to codify its prior guidance that a device is "produced by" an entity whenever that entity "exercises substantial responsibility for, or control over, any major stage of the process by which the device comes into existence," including its design, manufacturing, assembly, or development. Under the proposal, more than one entity could be deemed to have produced the same device. The Commission also asks whether to adopt the narrower exclusion proposed by Eagle Electronics, exclude design entirely, or adopt the substantially broader approach proposed by Telit Cinterion. In conjunction with this definition, the Commission proposes requiring an equipment-authorization applicant to submit a signed list identifying "any and all" entities that produced the device.[35]

INCOMPAS recognizes the Commission's legitimate interest in preventing a Covered List entity from evading an equipment-authorization prohibition by selling the same device under another company's name. A change in branding does not change the origin or security characteristics of the underlying equipment. But preventing that form of evasion does not require the Commission to classify every entity that contributed to a product's development as a producer of the finished device. The definition should only reach entities that exercise exclusive or primary ongoing control over the device's security-critical functions or exclusive authority

[35] *Third FNPRM* paras. 130–37; *id.* App. B (proposing 47 CFR § 2.911(d)(8)).

over its manufacturing specifications, not every participant in the extended process through which the product came into existence.

That limitation follows from the statutory framework. The Secure Networks Act makes a specific determination by an enumerated national-security source the predicate for including equipment or services on the Covered List. The Secure Equipment Act then prohibits authorization of equipment on that list. Where the underlying determination applies to equipment "produced by" a particular entity, the Commission may reasonably interpret that language to address rebranding and comparable attempts to evade the determination. It may not define "produced by" so expansively that the interpretation materially enlarges the equipment or entities reached by the underlying determination. Doing so would allow the Commission's implementing definition, rather than the enumerated source's determination, to establish the scope of the prohibition.[36]

The same statutory limitation applies to the proposed definition of "produced by." As the D.C. Circuit confirmed in *Hikvision*, the Commission may not implement the Secure Equipment Act through a definition that is unjustifiably broad or fails to comport with the statutory language incorporated into the Covered List.[37] The Commission therefore should ensure that "produced by" remains tied to the language and scope of each applicable national-security determination.

The proposed phrases "substantial responsibility" and "any major stage" do not provide that necessary boundary. Neither term identifies how much involvement is sufficient or distinguishes responsibility for the finished device from participation in an upstream activity.

---

[36] 47 U.S.C. § 1601(b)–(d); *Secure Equipment Act* § 2(a)(2), 135 Stat. at 423–24; National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3), 132 Stat. 1636, 1918–19.

[37] See *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948–50 (D.C. Cir. 2024); *Third FNPRM* para. 130 & n.254.

Equipment development can involve component suppliers, intellectual-property licensors, contract assemblers, reference-design providers, software developers, testing laboratories, and contributors to technical standards. Some of those parties may influence one aspect of development without retaining ongoing control over the device's security-critical functions or final manufacturing specifications. Treating each participant as a producer would collapse the distinction between producing the finished device and supplying an input or supporting service.

This uncertainty is particularly problematic because applicants must certify compliance with the Commission's equipment-authorization rules. A company could reasonably determine that an upstream participant did not "produce" its device, only for the Commission later to find that the participant exercised substantial responsibility for a major development stage. Regulated parties need fair notice of their obligations, especially when an ambiguous standard could lead to enforcement based on an allegedly inaccurate certification. Accordingly, any definition of "produced by" must provide a clear line, based on exclusive or primary ongoing control, that applicants can apply before signing and submitting an authorization application.

INCOMPAS recommends that the Commission define "produced by" to only reach an entity that exercises exclusive or primary ongoing control over the device's security-critical functions or exclusive authority over the device's manufacturing specifications. Security-critical control may include authority over firmware compilation and signing, update delivery, or cryptographic key management. This standard would focus on entities with the actual ability to introduce or exploit vulnerabilities in the device as deployed. It would not attribute production to every entity that contributed to an earlier stage of the device's creation or that performs physical assembly under another entity's direction.

That distinction is particularly important for products developed through partnerships. A company may incorporate partner-sourced components without ceding control over the security-critical functions of the finished device. The partner, in turn, may rely on its own suppliers or manufacturing facilities. An "any major stage" definition could attribute an entire product to an upstream entity based on that entity's limited contribution, even where another company exercises exclusive or primary ongoing control over the finished device's security posture. The appropriate inquiry is who retains that control, not whether an entity participated at some point in the extended development or production process.

An entity that merely licenses preexisting intellectual property, supplies a component, contributes to a technical standard, or provides another supporting service should not be treated as a producer on that basis alone. Similarly, originating-design intellectual property should not permanently attribute later products to the original designer after another company has assumed exclusive or primary ongoing control over their security-critical implementation. Historical participation in a predecessor product or underlying technology platform does not establish continuing control over the equipment submitted for authorization.

The Eagle Electronics proposal illustrates why originating design intellectual property should not be dispositive. Eagle describes circumstances in which another party controls the current design and firmware pathways, prevents unauthorized updates through cryptographic protections, and can demonstrate that the originating entity no longer has access to the device's logic-bearing subsystems. Those circumstances bear on whether the originating entity retains a practical ability to compromise the device. INCOMPAS's reliance on the Eagle proposal as support for an exclusion should not be understood as endorsing separate Commission mandates for independent security evaluation, supply-chain review, or any of the other safeguards Eagle

identifies. The controlling question should remain whether the originating entity retains exclusive or primary ongoing control over the device's security-critical functions.[38]

A device may have more than one producer only where each entity independently satisfies the applicable control standard with respect to a separate security-critical function, or where an entity separately holds exclusive authority over the final manufacturing specifications. Thus, one entity may exercise exclusive or primary ongoing control over one security-critical function and another entity over a different function. Two entities cannot both exercise exclusive control over the same function. The Commission should not aggregate several limited or upstream contributions and use their combined significance to classify each contributor as a producer. Otherwise, nearly every device developed through a multiparty supply chain could have numerous regulatory "producers," making the term too indeterminate to serve as a meaningful compliance standard.

The Commission also should reject the proposed requirement that applicants submit an unqualified, signed list of "any and all" producers. The proposal depends on the same undefined and overbroad conception of production that INCOMPAS opposes. Under the proposed definition, an applicant may not possess sufficient information to identify every entity that the Commission might later conclude participated in a major stage. The proposed rule contains no materiality threshold and would expose applicants to potential consequences for failing to identify an upstream participant that the applicant reasonably did not regard as a producer. The

[38] *Third FNPRM* paras. 131–34 & nn. 257–60; Letter from Mark Kvamme, Chairman, and Matt Wyckhouse, Board Member, Eagle Electronics, to Marlene H. Dortch, Secretary, FCC, at 3 (Oct. 15, 2025) (filed in ET Docket No. 21-232.

Commission should not impose an additional certification obligation whose scope cannot be determined at the time the certification is made.[39]

The Commission therefore should reject both the proposed "any major stage" definition and the associated requirement to submit a signed list of "any and all" producers. Any definition of "produced by" should be limited to entities that exercise exclusive or primary ongoing control over the device's security-critical functions or exclusive authority over its manufacturing specifications. The Commission also should exclude originating design intellectual property as a basis for producer status where the originating entity no longer exercises that control. This approach would address genuine rebranding or white-label evasion without extending the Covered List prohibition to upstream contributors that lack control over the security posture of the finished device.

VI. THE COMMISSION SHOULD NOT IMPOSE UNIVERSAL HBOM AND SBOM FILING REQUIREMENTS ON CERTIFICATION APPLICANTS

The *Third FNPRM* proposes that each certification applicant submit a written and signed HBOM and SBOM for the device for which authorization is sought. The proposed rules would require the applicant to identify all hardware, software, and firmware components; certify the submissions as true and correct; provide producer, production-location, and component-value information; and supplement the record at the request of the Commission or a Telecommunication Certification Body ("TCB"). Following grant, the responsible party would be required to update its submission within 30 days of a material change.[40] INCOMPAS opposes converting the equipment-authorization process into a universal supply-chain reporting program.

---

[39] *Third FNPRM* para. 135; *id.* App. B (proposing 47 CFR § 2.911(d)(8)); 47 CFR §§ 1.17, 2.911(d).

[40] *Third FNPRM* paras.139–46 & App. B (proposing 47 CFR §§ 2.911(d)(9)–(11), 2.931(f)).

If the Commission nevertheless moves forward with an HBOM or SBOM filing requirement, it should apply only to a clearly defined, higher-risk subset of equipment supported by an evidence-based assessment of identified supply-chain or national-security risk. A Covered List sector may inform that assessment where component origin is material, but sector status alone should not automatically trigger filing. Within that limited subset, required disclosures should extend only to critical components or components with a distinct nexus to the provision of RF communications.

The proposal also contains threshold ambiguities that the Commission must resolve before considering any filing mandate. Although paragraph 142 states that "all components" would be disclosed, proposed section 2.911(d)(10) specifies information for "each critical component" without supplying a generally applicable definition of that term. Paragraph 142 describes updates following "any changes," while proposed section 2.931(f) would require an update following a "material change." These differences affect the universe of reportable components, the frequency of updates, and an applicant's ability to certify compliance. They therefore cannot be left to informal guidance or case-by-case interpretation after a rule is adopted.

A. A Universal Filing Mandate Is Not Adequately Tethered to the Commission's Statutory Responsibilities

The Commission acknowledges that component origin, design and development locations, and supply-chain composition have not traditionally been treated as information relevant to equipment authorization and that its existing certification record was not designed to collect that information.[41] That history does not prevent the Commission from obtaining targeted

[41] *Id.* para. 140.

information necessary to administer the Covered List. It does, however, underscore the need to demonstrate why each proposed data element is reasonably necessary to perform a duty Congress assigned to the Commission.

The Secure Equipment Act directs the Commission not to review or approve applications involving equipment on the Covered List, while the Secure Networks Act establishes the determinations that support placement on that list. Those provisions create a direct statutory nexus between equipment authorization and equipment that has been found to pose an unacceptable national-security risk. They do not, on their face, direct the Commission to collect comprehensive supply-chain, production-location, and country-value information from every certification applicant, including applicants whose equipment has no identified connection to covered equipment or a Covered List determination. Section 302a of the Communications Act, meanwhile, authorizes rules governing devices capable of causing harmful interference. Sections 4(i) and 303(r) permit the Commission to implement responsibilities otherwise conferred by Congress, but do not constitute independent grants of authority to establish an untethered supply-chain reporting program.[42]

The Commission need not determine that it lacks authority to obtain any component information in every circumstance to reject the universal proposal. At a minimum, the Commission must identify the statutory responsibility served by each required field and establish a reasonable relationship between the information collected and an identifiable equipment-

[42] Secure Equipment Act § 2(a)(2); Secure Networks Act § 2(b)–(d), 47 U.S.C. § 1601(b)–(d); 47 U.S.C. §§ 154(i), 302a(a), 303(r); *Am. Libr. Ass'n v. FCC*, 406 F.3d 689, 698–700, 708 (D.C. Cir. 2005) (explaining that the Commission's ancillary authority must be tied to a statutorily mandated responsibility); *Comcast Corp. v. FCC*, 600 F.3d 642, 655–61 (D.C. Cir. 2010) (rejecting reliance on general policy statements and ancillary provisions without a sufficient connection to delegated authority).

authorization or Covered List determination. A universal requirement covering applicants with no demonstrated connection to covered equipment would not satisfy that standard.

The Odyssey Robot enforcement matter cited in the *Third FNPRM* does not bridge this gap. After the *Third FNPRM* was released, the FCC revoked Odyssey Robot LLC's equipment authorizations based on false statements and representations concerning whether unmanned aircraft systems "UAS" subject to a production-location-based Covered List entry were produced in the United States.[43] It may demonstrate the potential utility of obtaining producer or production-location information when those facts determine whether the specific equipment under review is covered. It does not demonstrate a need to collect a complete HBOM, SBOM, upstream producer directory, and country-value allocation for every device submitted for certification.

B. Conventional SBOM and HBOM Practices Do Not Support the Proposed Provenance and Valuation Requirements

SBOMs can be valuable cybersecurity tools. Existing federal frameworks generally use an SBOM to identify software components and their dependency relationships so that manufacturers, operators, and customers can identify and respond to vulnerabilities. Those frameworks do not treat an SBOM as an all-purpose record of where software was designed, where each contributor performed work, or what percentage of a finished device's value should be attributed to a particular country.[44] Distributed development, open-source contributions, and

---

[43] *Third FNPRM* para. 141; *Odyssey Robot LLC*, ET Docket No. 26-186, Order of Revocation, DA 26-839 (OET & PSHSB Aug. 11, 2026).

[44] Cybersecurity and Infrastructure Security Agency, *2026 Minimum Elements for a Software Bill of Materials (SBOM)* (July 29, 2026), https://www.cisa.gov/resources-tools/resources/2026-minimum-elements-software-bill-materials-sbom ("CISA 2026 Minimum Elements"); National Telecommunications and Information Administration, *The Minimum Elements for a Software Bill of Materials (SBOM)* (July 12, 2021), https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom ("NTIA Minimum Elements").

transitive dependencies make those concepts especially difficult to define consistently for software.

The proposed HBOM similarly would do substantially more than identify the hardware contained in a device. It would require applicants to determine the producer of each covered component, identify every location in which the component was designed or otherwise produced, allocate value among producers and locations, obtain extensive contact information, and certify the resulting submission as true and correct. That is a supply-chain provenance and valuation investigation, not simply the generation of a bill of materials.

The FDA example discussed in the *Third FNPRM* supports a targeted approach rather than the proposed universal mandate. Congress directed manufacturers of specified "cyber devices" to provide an SBOM addressing commercial, open-source, and off-the-shelf software components. The requirement is tied to the cybersecurity characteristics of a defined class of medical devices and does not convert the SBOM into a country-of-production or component-value report.[45] The FCC should employ comparable discipline by identifying the particular equipment and security risk that make component information necessary before requiring a submission.

The existence of free or inexpensive SBOM-generation tools does not establish that an applicant can produce a complete, validated, and continuously maintained submission satisfying the FCC's proposal at negligible cost. Automated tools can identify certain software artifacts available within a particular development environment. They cannot, by themselves, obtain

[45] Federal Food, Drug, and Cosmetic Act § 524B(b)(3), 21 U.S.C. § 360n-2(b)(3); Food and Drug Administration, *Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions* (Feb. 3, 2026).

information from upstream suppliers, resolve gaps involving proprietary or open-source code, validate sub-tier hardware information, assign production locations, or calculate the value attributable to each producer and country.

For the same reason, the *Third FNPRM's* preliminary cost estimates appear substantially understated. The Commission estimates that compliance for existing software would cost less than $5,000 per program, that an HBOM could require up to $10,000 in engineering and information-gathering costs per item of hardware equipment, and that approximately half of the equipment seeking authorization already satisfies the proposed requirements.[46] Those estimates do not appear to account for supplier outreach, contractual rights to obtain information, data validation, integration with product-development systems, governance and certification procedures, secure submission processes, or recurring maintenance. Member experience indicates that producing a complete SBOM for a single product can cost between $35,000 and $75,000, even before accounting for the proposed provenance, valuation, certification, and continuing-update obligations.

The burden would be particularly significant for complex compute and networking systems used in cloud and data-center environments. Such systems may incorporate thousands of components obtained through multi-tier global supply chains. An applicant may have substantial visibility into its direct suppliers but little practical ability to identify, validate, and continually monitor each upstream entity involved in producing a subcomponent. Delays in authorizing that equipment would also affect the networks and data centers on which the deployment of advanced AI services depends.

---

[46] *Third FNPRM* para. 143.

C. Any Alternative Requirement Must Reflect Applicants' Actual Access to Supply-Chain Information

Proposed section 2.911(d)(9)(iii) would require an authorized representative to certify that the HBOM and SBOM are "true and correct," and proposed section 2.911(d)(9)(iv) would allow the Commission or a TCB to demand documentation verifying completeness and accuracy.[47] An applicant should not be required to make an unqualified certification about information held by upstream suppliers and not reasonably available to it. That approach would create potential enforcement exposure even when an applicant has exercised appropriate diligence and reasonably relied on information furnished by its suppliers.

Any adopted requirement therefore must incorporate a reasonable-diligence standard. Applicants should be permitted to rely on supplier representations unless they know or have reason to know those representations are inaccurate. An applicant also should be permitted to identify information as unknown or not reasonably available after diligent inquiry. That approach would be consistent with existing SBOM practices, which recognize that complete information may not be available for every component, while preserving the Commission's ability to address knowing misrepresentations or failures to undertake reasonable inquiry.

The Commission also should make clear that only material changes can trigger an update. The narrative in paragraph 142 refers to updating an HBOM or SBOM within 30 days of "any changes," but proposed section 2.931(f) refers to "any material change."[48] The latter formulation should control, and the Commission should define materiality by reference to whether the change could affect the device's Covered List status or alter security-relevant information necessary to

---

[47] *Id.* App. B (proposing 47 CFR § 2.911(d)(9)(iii)–(iv)).

[48] Compare *id.* para. 142 (describing updates following "any changes"), with *id.* App. B (proposing 47 CFR § 2.931(f), which would require an update following "any material change").

an applicable authorization determination. Routine substitutions involving passive components or pre-vetted compliant suppliers should not generate new filings when they do not affect those determinations. Nor should ordinary software patches require a new submission unless they materially change the reportable software composition or the basis on which the Commission found the equipment eligible for authorization.

D. Any Collection Must Be Targeted, Secure, and Harmonized with Existing Standards

INCOMPAS urges the Commission to reject the proposed universal HBOM and SBOM filing mandate. The Commission has not demonstrated that requiring every certification applicant to submit detailed component information would materially advance an identifiable national security objective. Applying the mandate to equipment with no demonstrated connection to the Covered List would impose substantial costs and create security risks without a corresponding benefit.[49]

If the Commission nevertheless determines that some HBOM or SBOM information is necessary, any requirement should be limited at both the device and component levels. At the device level, the Commission should identify a clearly defined, higher-risk subset of equipment supported by an evidence-based assessment of an identified supply-chain or national-security risk. A device's presence within a Covered List sector may inform that assessment where component origin is material, but sector status alone should not automatically trigger an HBOM or SBOM filing requirement. Nor should sector status create a presumption that a device is covered, alter its authorization status, or require certification when the device otherwise qualifies for another authorization pathway.

[49] See *Third FNPRM* paras. 139–46 & App. B (proposing 47 CFR §§ 2.911(d)(9)–(11), 2.931(f)).

Within that limited device universe, disclosure should extend only to critical components or components with a distinct nexus to the provision of RF communications. "Critical components" should be defined narrowly by reference to the security risk addressed by the applicable Covered List entry. The requirement should exclude passive and mechanical components that neither perform a security-critical function nor have a distinct RF nexus. Requiring applicants to trace those components would increase compliance burdens without providing information material to determining whether the equipment implicates the applicable Covered List entry.[50]

For reportable components, the Commission should collect only the information necessary to determine whether the applicable Covered List entry reaches the equipment. Production-location and country-value information should not be added to an SBOM merely because an SBOM is otherwise required. Industry-standard SBOM frameworks identify software components and their dependency relationships; they are not designed to allocate product value among countries or identify every location in which software was designed or developed.[51] If the Commission establishes that production-location or country-value information is necessary in a particular context, it should develop a separate, workable methodology directed to that specific determination. These fallback limitations do not reflect INCOMPAS support for an HBOM or SBOM filing mandate. They represent the maximum appropriate scope if the Commission rejects INCOMPAS's primary recommendation and proceeds with a disclosure requirement.

[50] See *Third FNPRM* para. 142 & App. B (proposing 47 CFR § 2.911(d)(10)); Third R&O paras. 24–29, 31–35; CDA Comments at 2–3; CTIA Comments at 8–12; NCTA Comments at 4–5; Garmin Comments at 4–8.

[51] See CISA 2026 Minimum Elements at 4, 6, 19; NTIA Minimum Elements at 3- 4.

Any required submission would contain sensitive commercial and security information. A detailed inventory could disclose proprietary product architecture, supplier relationships, sourcing strategies, and potential points of attack. Public disclosure could cause competitive harm, while concentrating the information in a government repository would create an attractive target for attempted exfiltration. The Commission should keep any required submission outside the public Equipment Authorization System record, treat qualifying material as nonpublic commercial information under section 0.457(d), provide appropriate treatment under section 0.459, and follow section 0.461 before any contemplated disclosure.[52] Access should be limited to personnel who require the information to conduct the relevant authorization or Covered List review and protected through appropriate technical and administrative safeguards. If the Commission cannot provide legally enforceable assurance that required HBOM and SBOM submissions will remain nonpublic, subject only to disclosure required by law, it should not require applicants to submit those materials.

Before imposing any requirement, the Commission should harmonize its terminology and minimum fields with the work of CISA, NIST, and other federal agencies with relevant supply-chain and cybersecurity expertise. It should accept established machine-readable formats, including SPDX and CycloneDX, where those formats contain the information the Commission has lawfully required, rather than mandate a new FCC-specific artifact.[53]

---

[52] 5 U.S.C. § 552(b)(4); 47 CFR §§ 0.457(d), 0.459, 0.461; *Food Marketing Institute v. Argus Leader Media*, 588 U.S. 427, 434–40 (2019).

[53] CISA 2026 Minimum Elements; National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication 800-161 Rev. 1 (May 2022, updated Nov. 2024), https://doi.org/10.6028/NIST.SP.800-161r1-upd1; SPDX, *Specifications* (identifying SPDX 3.0 as the current version), https://spdx.dev/use/specifications/ (last visited Sept. 7, 2026); CycloneDX, *Specification Overview* (identifying CycloneDX 1.7 as the current version), https://cyclonedx.org/specification/overview/ (last visited Sept. 7, 2026)

The Commission should apply any requirement prospectively and allow sufficient implementation time. Existing authorizations should be grandfathered unless the Commission or an enumerated national-security source makes a specific determination concerning the affected equipment. A meaningful transition would be essential for applicants to establish supplier-reporting arrangements, implement necessary internal controls, and test secure submission processes.[54]

VII. THE COMMISSION SHOULD DECLINE TO IMPOSE BLANKET CERTIFICATION REQUIREMENTS ON ALL DEVICES WITHIN COVERED LIST SECTORS

The *Third FNPRM* proposes to amend section 2.907(c) to require every device within a "Covered List sector" to obtain authorization through the certification process, even if the device otherwise would qualify for the Supplier's Declaration of Conformity ("SDoC") process or would be exempt from equipment authorization. The proposal would apply to every device within the current sectors identified by the Commission, including UAS, UAS critical components, and routers, regardless of the device's producer, production location, or other characteristics.[55] INCOMPAS supports the use of certification where heightened Commission review is reasonably connected to an identified national-security risk. The Commission, however, has not justified requiring its most rigorous authorization process for every device that happens to fall within the same product sector as covered equipment.

A. Sector Status Alone Does Not Justify Eliminating Established Authorization Pathways

The Commission's existing rules require certification for equipment produced by an entity identified on the Covered List, even if that equipment otherwise would qualify for SDoC

---

[54] *Third FNPRM* para. 146.

[55] *Third FNPRM* paras.153–56 & App. B (proposing amendments to 47 CFR §§ 2.906(d), 2.907(c)).

or an exemption.[56] That requirement reflects a direct relationship between the identity of the producer, the determination underlying the producer's placement on the Covered List, and the Commission's obligation to prevent authorization of covered equipment.

Production-location-based Covered List determinations operate differently. Those determinations identify equipment by reference to a product category and a specified geographic nexus. A device can therefore fall within the broader product sector without itself satisfying the conditions that make equipment covered. A domestically produced or conditionally approved router, for example, may be within the router sector but outside the applicable Covered List entry. The proposal nevertheless would require that device to undergo certification solely because it shares a product category with covered routers.

The Secure Equipment Act directs the Commission not to review or approve applications involving equipment on the Covered List. It does not require the Commission to subject every non-covered device within a related product category to the certification process.[57] Although the Commission has authority to establish equipment-authorization procedures, it must explain why the distinguishing feature it selected, membership in a broadly defined sector, reasonably corresponds to the regulatory problem the proposed rule is intended to address. The existence of covered equipment within a sector does not, without more, establish that all other equipment within that sector requires the same degree of premarket review. A final rule must articulate a

[56] *Id.* para. 153; 47 CFR § 2.907(c).

[57] Secure Equipment Act § 2(a)(2); Secure Networks Act § 2(b)–(d), 47 U.S.C. § 1601(b)–(d).

rational connection between the risks identified in the record and the scope of the regulatory response.[58]

The existing SDoC process is not an exemption from substantive compliance. It places responsibility on a U.S.-based responsible party to ensure that the equipment complies with the applicable technical standards, requires appropriate testing or other compliance demonstrations, and requires the responsible party to provide specified compliance information.[59] The Commission adopted that pathway because certain types of equipment can be regulated effectively without an application to and affirmative grant from a TCB. Nothing in the *Third FNPRM* demonstrates that compliant equipment becomes more likely to cause harmful interference or present a national-security risk merely because another device within the same general product sector is covered.

Certification would impose materially different obligations. An applicant must prepare and submit an application, supporting documentation, and applicable measurement data for review by a TCB before marketing the equipment. Extending that process to devices currently exempt from authorization would create a new premarket review requirement where none presently exists. The *Third FNPRM* does not explain how all certification requirements would apply to those otherwise-exempt devices or what additional technical showing a TCB would be expected to evaluate.

The proposal also could substantially increase the number of certification applications without establishing that the Commission and TCBs have the capacity to review them without

---

[58] 5 U.S.C. § 706(2)(A); *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

[59] 47 CFR §§ 2.906, 2.1074, 2.1077.

delay. Indeed, the Commission asks whether the rule would add approximately 10,000 or 100,000 products annually, or some other number.[60] That unanswered question is material. Before expanding certification, the Commission should determine the number and types of affected devices, the available review capacity, and the likely effect on authorization timelines. Otherwise, the rule could delay lawful equipment without improving the Commission's ability to identify covered equipment.

Those delays would be particularly consequential if an expanding definition of a Covered List sector reached equipment used in professionally managed communications and data-center environments. The Commission's current router definition is limited to consumer-grade networking devices primarily intended for residential use, and its guidance expressly excludes industrial, enterprise, and military equipment.[61] The Commission should preserve that boundary and make clear that the certification proposal does not reach enterprise, data-center, or infrastructure networking equipment. Applying consumer-focused certification requirements to that equipment could delay deployment of the computing and network infrastructure needed to support American AI leadership without addressing the risks identified in the router determination.

B. The Commission Can Address Potential Circumvention Through More Targeted Measures

The Commission expresses concern that a device within a Covered List sector might incorporate an authorized modular transmitter and rely on that transmitter's FCC identification

---

[60] *Third FNPRM* para. 156.

[61] *Third FNPRM* paras. 204–06; FCC, *FAQs on Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries*, https://www.fcc.gov/faqs-recent-updates-fcc-covered-list-regarding-routers-produced-foreign-countries (updated May 12, 2026) (stating that the router definition does not include "[i]ndustrial, enterprise, or military equipment").

number without separately undergoing equipment authorization. According to the *Third FNPRM*, that framework could allow a host device that is actually covered equipment to avoid the review that otherwise would reveal its covered status.[62] That is a legitimate issue for the Commission to examine, but the proposed solution sweeps beyond the identified concern.

Equipment that actually falls within a Covered List entry remains subject to the Commission's prohibitions regardless of whether it otherwise would qualify for certification, SDoC, or an equipment-authorization exemption. The potential enforcement gap therefore concerns the Commission's ability to identify whether a particular host device is covered; it does not establish that every host device in the same sector requires a complete certification proceeding.

If the Commission concludes that some form of premarket review is necessary, it should identify the particular equipment and circumstances that create the risk and tailor the requirement accordingly. It should not presume that each future production-location-based addition to the Covered List automatically justifies certification of every non-covered device within the associated sector. Each sector presents different equipment characteristics, supply chains, deployment environments, and existing oversight mechanisms. The Commission should develop a sector-specific record and provide an opportunity for affected parties to address those considerations before changing the authorization pathway for devices that are not themselves covered equipment.

The Commission's recent experience with production-location-based entries reinforces the need for that approach. Since establishing those entries, the responsible national-security

[62] *Third FNPRM* paras. 155–56; 47 CFR § 2.903(a)–(c).

agencies have issued further determinations and granted Conditional Approvals for particular equipment, and the Commission has implemented those determinations by clarifying and modifying the scope of at least one sector-based entry.[63] Those actions may reflect appropriate refinement as agencies obtain additional information, but they also demonstrate why an authorization rule should not automatically attach permanent regulatory consequences to the broadest initial description of a product sector.

The Commission also should preserve workable treatment for equipment that has received a Conditional Approval or comparable federal review demonstrating that it does not present the risk addressed by the relevant Covered List entry. Requiring full certification solely because the equipment remains within the broader sector would discount the individualized federal determination and duplicate review without an evident security benefit. The Commission should likewise consider whether existing federal oversight provides a sufficient basis to retain SDoC eligibility for particular closed-loop commercial operations.

Any certification expansion should apply prospectively and include a meaningful implementation period. Existing lawful authorizations should remain valid absent a specific determination addressing the equipment or an established basis for modification, revocation, or withdrawal under the Commission's rules. Manufacturers also should have sufficient time to adjust testing arrangements, compliance systems, and product-development schedules. These protections would allow the Commission to address demonstrated risks without disrupting the

[63] See, e.g., *FCC's Public Safety and Homeland Security Bureau Announces Conditional Approval and Exemption of Certain Uncrewed Aircraft Systems and Routers from FCC Covered List*, Public Notice, DA 26-875 (PSHSB Aug. 21, 2026); *Following New National Security Determination, FCC Announces Modification of Power Inverters Entry on the Covered List*, Public Notice, DA 26-870 (PSHSB Aug. 20, 2026).

availability of lawful equipment or delaying the deployment of communications and AI infrastructure.

VIII. THE COMMISSION SHOULD PRESERVE WORKABLE IMPORTATION, TESTING, EVALUATION, AND R&D PATHWAYS

The *Third FNPRM* proposes to exclude covered equipment from the generally applicable importation conditions in section 2.1204(a) and establish a separate set of conditions under which covered equipment could enter the United States without a valid equipment authorization. Under proposed section 2.1204(c), covered equipment could be imported if it falls within one of several specified categories. For testing, evaluation, or product development, the proposal would allow importation of up to 40 units and would require written approval from the Chief of the Office of Engineering and Technology ("OET") for a greater quantity.[64]

INCOMPAS reinforces its support for appropriate safeguards against the unauthorized commercial distribution of covered equipment. Those safeguards, however, should not prevent U.S. companies from obtaining the equipment needed to evaluate security risks, develop compliant products, or advance American AI and robotics capabilities. The Commission should preserve an importation pathway that accommodates legitimate development programs while maintaining controls against unauthorized marketing.

A. The Forty-Unit Default Would Not Accommodate Many Legitimate Testing and Development Programs

The Commission's existing rule permits importation of up to 4,000 units of an unauthorized radiofrequency device for testing and evaluation, product development, or evaluation of suitability for marketing. The devices may not be offered for sale or marketed, and the OET Chief may approve a greater quantity. Distinct models and separate generations of a

[64] *Third FNPRM* paras.159–67 & App. B (proposing 47 CFR § 2.1204(c)(2)).

model under development are counted as separate devices.[65] The *Third FNPRM* proposes a substantially lower default for covered equipment because the Commission considers 4,000 units unnecessarily high and because covered equipment cannot lawfully be marketed in the United States.[66]

INCOMPAS does not contend that covered equipment should be imported to evaluate its suitability for marketing in a market where its sale is prohibited. Testing and product development serve different purposes, however. Companies may need covered equipment to determine whether it presents a vulnerability, evaluate interoperability with communications networks, develop replacements, or validate protective controls. The inability to market the equipment does not eliminate those legitimate uses.

INCOMPAS members report that current testing and development programs can require more than 40 units of a model. A single program may involve concurrent work at geographically dispersed laboratories, destructive or stress testing, testing across successive software configurations, and evaluation in different operational environments. AI and robotics development can require multiple devices to generate a sufficiently varied body of performance data. A 40-unit default could therefore be exhausted before a company completes a legitimate controlled testing program.

The Commission has not provided an empirical basis for concluding that 40 units will ordinarily be sufficient. The *Third FNPRM* cites the Commission's experience with device testing but expressly asks whether a larger quantity is needed.[67] The Commission should evaluate

---

[65] 47 CFR § 2.1204(a)(3)(i)–(ii).

[66] *Third FNPRM* para. 161.

[67] *Id.*

evidence from actual development programs before establishing a numerical threshold that could constrain U.S. research. Unless the record supports 40 units, the Commission should retain a higher default threshold appropriate for controlled testing and product development.

The Commission also should reconcile an ambiguity between the *Third FNPRM*'s discussion and the proposed rule. Paragraph 161 discusses a limit of 40 units "for a given model," while proposed section 2.1204(c)(2) refers only to equipment "imported in a quantity of 40 or fewer units."[68] The proposed rule does not say whether the limit applies per distinct model, per generation of a model, per shipment, per importer, or across an entire development program. The current rule expressly treats distinct models and separate generations as separate devices. Any final rule should preserve that approach and state clearly how the threshold will be calculated.

If the Commission retains a 40-unit default, the alternative OET-approval pathway must be prompt and administrable. The Commission should publish the information needed to support a request, identify the safeguards it will consider, and provide a predictable process for obtaining a written decision before importation.

A higher threshold or streamlined approval process should remain subject to appropriate controls against unauthorized marketing or deployment.

B. Product Development Should Expressly Include Software and AI-Model Development

The phrase "product development" in proposed section 2.1204(c)(2) is broad enough to encompass more than modification of the imported hardware itself, but the *Third FNPRM* does not explain its intended scope. The Commission should clarify that covered equipment may be

[68] Compare *id.* para. 161, with *id.* App. B (proposing 47 CFR § 2.1204(c)(2)).

imported for the development and validation of software, AI models, and security protections, even when the resulting software or model will be deployed on different, otherwise lawful hardware.

That clarification is especially important for robotics. Developers train and evaluate robotics models by observing how physical systems respond to different environments and tasks. Simulation can supplement that work but may not reproduce every physical interaction or operating condition. Access to physical hardware allows developers to identify unsafe behavior, test for vulnerabilities, and generate the real-world data needed to improve U.S.-developed models. A rule that allows examination of a device's hardware but prohibits using that same device to validate the software or model controlling it would draw an artificial distinction that does not reflect how these systems are developed.

The Commission therefore should state that permissible product development includes software validation, AI-model testing, cybersecurity research, and controlled collection of physical-world training data. Those activities should remain subject to the prohibition against offering the imported equipment for sale or otherwise placing it into commercial distribution. The importer also should employ controls appropriate to the risk presented by the equipment, including isolation from sensitive networks where warranted. These limitations would permit American developers to learn from and test the equipment without authorizing its commercial deployment.

This clarification would advance the Commission's national security objectives. Testing covered equipment can help U.S. companies identify potential attack vectors, develop mitigations, and design compliant alternatives. In the AI and robotics context, access to physical systems can also support development of U.S.-controlled software and models that ultimately

operate on domestic or trusted hardware. Preventing that research could impair the very domestic capabilities that the Commission's supply-chain initiatives seek to strengthen.

C. Conditional Approvals and Waivers Must Remain Available Where the Risk Can Be Controlled

Importation relief also should account for equipment that has received a Conditional Approval or comparable determination from an authorized national-security agency. A Conditional Approval may establish restrictions that address the risk presented by otherwise-covered equipment. Where the approval authorizes importation for specified purposes, the Commission's rules should recognize that determination rather than impose a conflicting prohibition.[69]

The Commission should likewise retain its ability to waive the numerical limit or another import condition for good cause under section 1.3. A waiver may be appropriate when a company demonstrates a legitimate need for a larger quantity, identifies the facilities and parties that will control the equipment, and establishes protections against unauthorized distribution.[70] Because case-by-case waivers can require significant time and resources, however, they should supplement—not replace—a workable generally applicable testing and product-development pathway.

An allied-country R&D safe harbor could provide an additional protection for controlled research and development involving equipment or components sourced from TAA-compliant or

---

[69] See FCC Covered List; *Third FNPRM* para. 184 & n.333; see also, *FCC's Public Safety and Homeland Security Bureau Announces Conditional Approval and Exemption of Certain Uncrewed Aircraft Systems and Routers from FCC Covered List*, Public Notice, DA 26-875 (PSHSB Aug. 21, 2026); *Following New National Security Determination, FCC Announces Modification of Power Inverters Entry on the Covered List*, Public Notice, DA 26-870 (PSHSB Aug. 20, 2026).

[70] 47 CFR § 1.3; see also *Third FNPRM* paras. 160–61 (proposing that the OET Chief retain authority to approve quantities exceeding the generally applicable limit).

other allied countries. Any such safe harbor should supplement—not displace—the generally available, streamlined OET process and workable numerical threshold described above.

IX. THE COMMISSION SHOULD ADOPT A NARROW DEFINITION OF "PRODUCED IN A FOREIGN COUNTRY" THAT TARGETS FOREIGN-ADVERSARY RISK AND RESPECTS THE UNDERLYING NATIONAL-SECURITY DETERMINATION

The Commission seeks comment on how to interpret "produced in a foreign country" when that phrase appears in a national-security determination underlying a Covered List entry. It tentatively proposes to treat equipment as produced in a foreign country whenever the equipment fails to qualify as a "domestic end product" under the Federal Acquisition Regulation ("FAR"). The Commission also asks whether it should use the Federal Trade Commission's ("FTC") standard for an unqualified "Made in USA" claim, treat foreign design or development activity as sufficient, or adopt a narrower rule based on trade law's country-of-origin principles.[71]

INCOMPAS supports a clear and administrable definition. Neither the FAR domestic-content test nor the FTC's consumer-labeling rule, however, was designed to identify national-security risk. Importing either standard into the equipment-authorization program would conflate a product's eligibility for a procurement preference or an unqualified advertising claim with the separate question whether the product was meaningfully produced in a location relevant to an identified security threat.

The Commission's interpretation also must remain faithful to the determination issued by the relevant enumerated source. The Secure Networks Act requires the Commission to place equipment on the Covered List based exclusively on specified national-security determinations

[71] *Third FNPRM* paras. 197–201.

and to update the list in response to changes in those determinations.[72] The Commission may clarify an ambiguous term to administer its rules, but it should not expand or narrow the substantive scope of an underlying determination in a manner inconsistent with the issuing agency's intent. If the meaning of "produced in a foreign country" cannot be resolved from the determination itself, the Commission should obtain clarification from the issuing agency rather than adopt an interpretation that effectively rewrites that determination.

A. Procurement and Consumer-Labeling Standards Are Poor Proxies for National-Security Risk

The *Third FNPRM's* description of the FAR standard requires refinement. FAR 25.101 establishes a two-part test for manufactured domestic end-products. The article must be manufactured in the United States, and, unless an applicable exception applies, the cost of domestic components must exceed the prescribed percentage of the cost of all components.[73] The current percentage is 65% for items delivered during calendar years 2024 through 2028 and increases to 75% beginning in 2029. The domestic-component test is also waived for many commercially available off-the-shelf ("COTS") items, subject to an exception for products consisting wholly or predominantly of iron or steel.[74]

Those features illustrate why the FAR is not an appropriate definition of where equipment was "produced" for Covered List purposes. The FAR implements the Buy American statute in federal procurement. Its thresholds determine whether an agency may treat an offered

[72] Secure Networks Act § 2(b)–(d), 47 U.S.C. § 1601(b)–(d).

[73] 48 CFR §§ 25.003, 25.101(a)(1)–(2).

[74] 48 CFR § 25.101(a)(2)(i)–(ii).

product as domestic when applying procurement preferences. They do not determine whether the product poses an unacceptable national security risk.

Using that procurement test also could produce arbitrary results in the equipment-authorization context. The same device could change from "domestic" to "foreign-produced" solely because the FAR percentage increases in 2029, even though the device's design, manufacturing process, producer, and security characteristics remain unchanged. Application of the COTS waiver could produce a different classification for commercially available equipment than for otherwise comparable non-COTS equipment. Those distinctions may serve federal procurement policy, but the *Third FNPRM* does not explain why they should control national-security treatment under the Covered List.

The FAR approach also would capture U.S.-designed products manufactured through trusted global supply chains whenever the finished device fails the U.S.-manufacturing prong or the applicable component-cost test. INCOMPAS members rely on suppliers located in the United States and allied countries to produce communications, computing, and data-center equipment. Treating all equipment that does not satisfy a domestic procurement preference as "produced in a foreign country" would fail to distinguish trusted allied production from production associated with an identified foreign-adversary risk.

The FTC's "Made in USA" standard is equally unsuitable. The FTC rule governs unqualified U.S.-origin claims on product labels. Such a claim generally may be made only when final assembly or processing occurs in the United States, all significant processing occurs here, and all or virtually all ingredients or components are made and sourced domestically.[75] The rule

[75] Made in USA Labeling Rule, 16 CFR § 323.2(a); Federal Trade Commission, *Complying with the Made in USA Standard* (July 2, 2024), https://www.ftc.gov/business-guidance/resources/complying-made-usa-standard.

protects consumers from deceptive origin claims; it does not define foreign production for national-security regulation.

A product that cannot carry an unqualified "Made in USA" label is not necessarily produced by an untrusted entity or in a country that presents an identified security concern. The product may have been substantially transformed in the United States while incorporating meaningful content from a trusted allied country. It also may qualify for a truthful, qualified U.S.-origin claim even though it fails the FTC's more demanding standard for an unqualified claim. Treating every product that cannot make the unqualified claim as foreign-produced would convert a consumer-protection standard into a security classification that the FTC rule was never intended to supply.

Likewise, the Commission should reject a test under which any foreign design or development activity makes a device foreign-produced. The *Third FNPRM* asks whether the work of any foreign-based employee or some number or percentage of foreign-based employees should determine the device's production location.[76] Such a test would be difficult to administer in globally distributed engineering organizations and would not reliably identify the party or location that controls the security characteristics of the finished device.

As discussed above regarding the definition of "produced by," design activity should matter only when it places exclusive or primary ongoing control over the finished device's security-critical functions, or exclusive authority over its manufacturing specifications, in a foreign entity. An employee's location does not establish that the employee or a foreign entity

[76] *Third FNPRM* paras. 198–99.

exercises that control. The Commission should not classify an entire device as foreign-produced because a foreign-based employee made a limited contribution to a global development process.

B. A Substantial-Transformation Framework Provides a More Appropriate Starting Point

A country-of-origin analysis grounded in substantial transformation provides a better starting point. Customs law generally identifies a product's country of origin as the country of manufacture, production, or growth. When work or materials from more than one country are involved, additional processing must effect a substantial transformation for the second country to become the country of origin.[77] Courts generally ask whether the process results in a new and different article with a distinctive name, character, or use.[78]

That framework focuses on where the relevant finished article came into being rather than asking whether every component was sourced domestically. It therefore better reflects the ordinary meaning of where a device was produced and is less likely to treat the presence of an allied-country component as dispositive. It also preserves the distinction between producing the finished device and supplying an input to that device.

Substantial transformation is nevertheless a fact-specific standard, not a complete rule ready for incorporation without further guidance. Courts and Customs and Border Protection ("CBP") consider the nature and complexity of the processing, whether components retain predetermined uses, and which operations impart the finished article's essential character.[79]

---

[77] 19 U.S.C. § 1304; 19 CFR § 134.1(b).

[78] *Anheuser-Busch Brewing Ass'n v. United States*, 207 U.S. 556, 562 (1908).

[79] *Energizer Battery, Inc. v. United States*, 190 F. Supp. 3d 1308, 1316–20, 1324–25 (Ct. Int'l Trade 2016) (explaining the fact-specific substantial-transformation inquiry and concluding that the assembly at issue did not substantially transform the imported components).

Different origin regimes can also apply different rules to the same product depending on the governing statute or trade program.

The Commission therefore should identify the precise substantial-transformation framework it intends to use. It should explain how that framework applies to electronic devices assembled from globally sourced components and how it treats device-specific firmware or other processing that determines the finished product's functionality.

The definition also should operate at the level of the finished device addressed by the national-security determination. A component's origin should not determine the production location of the finished device unless the underlying determination expressly reaches that component or the component undergoes no substantial transformation when incorporated into the finished product. This limitation is necessary to prevent a definition of production location from becoming a de facto component prohibition broader than the Covered List entry itself.

Determining where a device was produced is also distinct from deciding whether that production location presents sufficient risk to trigger Covered List consequences. The substantial-transformation inquiry addresses origin. The underlying national-security determination must establish the connection between that origin and the unacceptable risk identified by the enumerated source. The Commission should not use a country-of-origin definition to supply a risk determination that the enumerated source did not make.

The Commission asks whether its interpretation should apply to existing and future production-location-based Covered List entries.[80] Any definition should apply prospectively unless the enumerated source expressly confirms that the definition reflects the intended scope of

[80] *Third FNPRM* para. 201.

an existing determination. A new FCC interpretation should not retroactively alter the treatment of equipment that manufacturers imported, developed, or submitted for authorization in reasonable reliance on the prior language and guidance. For future entries, the Commission should publish the operative definition with sufficient notice for affected companies to determine how it applies to their products and supply chains.

X. THE COMMISSION SHOULD NOT ADOPT A UNIVERSAL REGISTRATION REQUIREMENT FOR SDOC DEVICES

The Commission proposes to require every device authorized through the Supplier's Declaration of Conformity ("SDoC") process to be registered before marketing, assigned a Commission-issued identifier, publicly listed, and subject to new display requirements.[81] INCOMPAS respectfully urges the Commission not to adopt that universal mandate. It would impose a new federal filing obligation across broad categories of compliant equipment without demonstrating that the absence of an FCC registration record has created a material enforcement or national-security gap. If the Commission nevertheless proceeds, any registration requirement should be confined to a clearly defined, higher-risk subset of equipment supported by an evidence-based assessment. Equipment's presence within a Covered List sector may serve as one possible screen for identifying such a subset, but it should not automatically trigger registration.

SDoC is not an exemption from the Commission's technical rules. The responsible party must make the required measurements or complete other procedures acceptable to the Commission, ensure that the equipment complies with the applicable technical standards, retain adequate identification records, and provide prescribed compliance information with the

[81] *Third FNPRM* paras. 211–15 & App. B (proposing 47 CFR § 2.906(e)–(f)).

product.[82] The distinguishing feature of SDoC is that the responsible party may demonstrate compliance without submitting an application for Commission approval before marketing. That distinction reflects the Commission's longstanding judgment that automatic filing would add administrative burdens without necessarily providing additional assurance of compliance.[83]

The *Third FNPRM* points to the Commission's removal of twenty-eight entities from the equipment-authorization system based on improper conduct or unacceptable national-security risk.[84] But it does not identify how many of those actions involved equipment relying on SDoC, whether the absence of an SDoC registration record impeded detection or enforcement, or how universal registration would have prevented the underlying conduct. A registration record establishes that information was submitted; it does not establish that required measurements were properly performed, that a laboratory was competent, or that a device's supply chain presents no security concern. The Commission's improved technical ability to maintain a database likewise establishes that registration is possible, not that it is necessary or appropriately applied to every SDoC device. The Commission must supply a rational connection between the problem identified in the record and the breadth of the remedy it ultimately adopts.[85]

Existing safeguards also address the equipment presenting the most clearly identified risks. Covered equipment may not receive equipment authorization through SDoC, and equipment produced by an entity identified on the Covered List is likewise ineligible for that

---

[82] 47 CFR §§ 2.906(a)–(b), 2.945, 2.1074(a), 2.1077.

[83] *Amendment of Parts 2 and 15 of the Commission's Rules to Deregulate the Equipment Authorization Requirements for Digital Devices*, ET Docket No. 95-19, Report and Order, 11 FCC Rcd 17915 (1996); *Third FNPRM* para. 211.

[84] *Third FNPRM* para. 212.

[85] *Motor Vehicle Manufacturers Association of the United States, Inc. v. State Farm Mutual Automobile Insurance Co.,* 463 U.S. 29, 43 (1983).

process.[86] The Commission retains authority to request representative data or a sample unit, inspect required records, and pursue enforcement where a responsible party fails to comply with the applicable rules.[87] The Commission should use those authorities against identified misconduct rather than convert SDoC into a universal registration program for equipment that has not been associated with a demonstrated security concern.

That distinction is especially important to INCOMPAS members building and operating the networks, cloud facilities, and data centers that enable artificial-intelligence and other advanced computing services. Members rely on the SDoC pathway for categories of information-technology equipment incorporated into servers, storage systems, network infrastructure, power-management systems, and supporting peripherals. These products may be deployed across numerous facilities and may have multiple configurations or model variants even when their relevant RF characteristics remain unchanged. Requiring a separate Commission filing for every affected SDoC model would require changes to product-release workflows, labeling and packaging controls, inventory systems, online product records, and global compliance databases. Those recurring obligations would slow the introduction and deployment of routine infrastructure equipment without a corresponding showing of national-security benefit.

The proposed FCC-issued identifier also would substantially duplicate information already required by the Commission's rules. Section 2.1074 requires the responsible party to provide unique product identification and maintain records sufficient to identify the equipment. Section 2.1077 requires the accompanying compliance information statement to identify the product by name and model number, state the applicable compliance information, and identify a

[86] 47 CFR §§ 2.903(a), 2.906(d); *Third FNPRM* para. 212.

[87] 47 CFR §§ 2.906(a)(2), 2.938, 2.945.

responsible party located in the United States.[88] The Commission has not identified a traceability problem that those existing identifiers cannot address or explained why a second, FCC-specific number would materially improve enforcement.

INCOMPAS therefore opposes requiring a new FCC-issued identifier for SDoC devices. If the Commission nevertheless requires a public record for a clearly defined, higher-risk subset of SDoC equipment, it should adopt a manufacturer-hosted model. The responsible party or manufacturer should maintain a publicly searchable SDoC record indexed by its name together with the device's existing model number. The Commission should not require a duplicative FCC-hosted registration or compel manufacturers to assign another identifier or change product labels, packaging, inventory records, and online listings solely to display a new FCC number.

Nor should an SDoC registration system become a vehicle for collecting HBOMs, SBOMs, component-producer information, or production-location data. As explained above, those disclosures would expose sensitive supply-chain information, create substantial compliance and cybersecurity risks, and require continuing updates that bear little relationship to the purpose of SDoC registration. If the Commission proceeds at all, the registrant should be required to provide no more than the information already contained in the section 2.1077 compliance statement. The Commission should not use registration to expand the responsible party's obligations beyond those that apply under the existing SDoC rules.

The Commission should also avoid creating duplicative obligations for composite devices. Section 2.1077(b) already specifies the compliance information that must accompany an

[88] 47 CFR §§ 2.1074(a), 2.1077(a).

assembled product containing components authorized through SDoC, certification, or both.[89] Any targeted registration requirement should permit the responsible party to rely on that existing documentation and, where applicable, cross-reference the existing FCC ID of a certified component. It should not require a new component-level map, duplicate registrations for incorporated modules, or additional supply-chain disclosures.

If the Commission nevertheless concludes that additional public information is necessary, any registration requirement should be limited to a clearly defined, higher-risk subset of equipment supported by an evidence-based assessment demonstrating a specific compliance, enforcement, or national-security concern and explaining how registration would address that concern.[90] If, as INCOMPAS recommends in the preceding section, the Commission preserves SDoC eligibility for devices within a Covered List sector, it could consider narrowly targeted registration for a demonstrably higher-risk subset of those devices as a less burdensome alternative to categorical certification.

Covered List-sector status should serve only as one possible screen for identifying equipment that may warrant further assessment, not as an automatic registration trigger. Before imposing registration based on that screen, the Commission should identify record evidence showing that the defined subset presents a heightened risk and that registration would materially assist the Commission in addressing it. The mere fact that a device falls within the same general product sector as covered equipment does not establish that the device should be registered.

---

[89] 47 CFR § 2.1077(b); *Third FNPRM* para. 213.

[90] *Third FNPRM* para. 213.

Any fallback record that survives that analysis must remain purely ministerial. Posting the prescribed SDoC record on the responsible party's or manufacturer's publicly searchable website should satisfy the obligation, with no separate Commission filing, substantive Commission review, processing queue, or hold on marketing. The fallback record should not become an independent basis for suspending or prohibiting a product that otherwise complies with the Commission's rules. Any enforcement action should continue to rest on a violation of an applicable substantive or procedural requirement.

Any new registration requirement should apply only prospectively after the Commission has finalized the relevant specifications, interfaces, and data standards. Products already lawfully marketed through SDoC, existing inventory, and existing online listings should be grandfathered. The Commission should provide sufficient implementation time and a meaningful opportunity to correct good-faith clerical or data-quality errors before any enforcement consequence attaches.

XI. ONLINE-MARKETPLACE OBLIGATIONS SHOULD REFLECT CONTROL OVER COMPLIANCE INFORMATION

The Commission should ensure that any new obligations governing SDoC devices reflect the information and control available to each participant in the distribution chain. In the *Third R&O*, the Commission adopted requirements for online display of FCC identifiers associated with certified equipment. Those rules distinguish between marketplaces that sell their own products or have physical access to or take title to a third-party product and marketplaces that merely host a listing without access to the underlying device.[91] The *Third FNPRM* now proposes to extend related collection, verification, record-retention, and display obligations to devices

[91] *Third R&0* paras. 62–76 & App. A (adopting 47 CFR § 2.803(c)). In particular, section 2.803(c)(2) applies a different verification standard where the marketplace neither has physical access to nor takes title to the third-party seller's device.

authorized through SDoC and to devices asserted to be exempt from equipment authorization.[92] INCOMPAS opposes new requirements that would make retailers or online marketplaces independently verify SDoC compliance information. The Commission should preserve and strengthen the control-based distinctions reflected in its rules for certified equipment rather than impose uniform obligations on materially different retail and marketplace models.

The manufacturer, importer, or other responsible party remains best positioned to determine the authorization status of a device and the accuracy of the supporting compliance information. That party designs or imports the product, selects the applicable authorization procedure, conducts or obtains the necessary testing, and maintains the records required by the Commission's rules. For an SDoC device, the responsible party must provide a compliance information statement identifying the product and the U.S.-based party responsible for compliance.[93] An online marketplace that does not manufacture, import, possess, or take title to the device generally lacks access to the product, its technical specifications, its test results, and the facts needed to determine whether the device requires certification, may rely on SDoC, or qualifies for an exemption.

The Commission therefore should not require a retailer or online marketplace that lacks physical access to the device to verify SDoC compliance information or make an independent technical determination regarding the product's authorization status. Determining whether a particular device qualifies for SDoC or an exemption may require an analysis of its circuitry, operating characteristics, intended use, and applicable technical standards. A marketplace cannot reliably perform that analysis from a merchant's product description or photographs. Requiring it

---

[92] *Third FNPRM* para. 168; *id.* paras. 214–15 & App. B (proposed 47 CFR § 2.804(c)).

[93] 47 CFR §§ 2.1074, 2.1077; *Third FNPRM* para. 214.

to do so would transfer substantive equipment-compliance responsibility from the party that controls the relevant facts to an intermediary that ordinarily does not possess them. The predictable result would be inconsistent classification and removal of lawfully marketed products, with disproportionate consequences for small sellers and purchasers seeking lawful communications or computing equipment.

If the Commission nevertheless imposes a limited collection-and-display obligation on a third-party marketplace that neither possesses nor takes title to the product, the obligation should be confined to collecting prescribed information supplied by the responsible party or seller and displaying that information accurately. The marketplace should be permitted to rely reasonably on a facially valid submission and seller certification unless it has actual knowledge that the information is materially false or fails to act after receiving sufficiently specific notice of a defect. This fallback would be consistent with the protection the Commission has already adopted for certified devices: a marketplace without physical access to the product is not liable for an inaccurate FCC identifier supplied by a third-party seller if the marketplace reasonably verifies that the identifier exists in the Equipment Authorization System ("EAS") and requires the seller to certify the information's accuracy.[94]

If the Commission adopts any limited SDoC or exempt-device obligation, it should also provide a clear, objective safe harbor based on reasonable procedures. A marketplace should qualify by requiring the seller or responsible party to provide the applicable compliance statement or exemption attestation, preserving that submission for the required period, accurately displaying the prescribed information, and acting within a reasonable period after obtaining

[94] *Third R&O* para. 74 & App. A (adopting 47 CFR § 2.803(c)(2)).

actual knowledge or receiving a specific Commission notice that the information is materially defective. An isolated clerical error, database outage, or inaccurate statement supplied by a third party should not subject a marketplace to liability where the marketplace followed the prescribed process in good faith. Nor should a missing or temporarily unverifiable record automatically require suppression of a listing before the seller receives notice and a reasonable opportunity to cure, except where the Commission identifies covered equipment, an otherwise unauthorized device, or another concrete and urgent risk.

The proposed verification requirement is unworkable for reasons that a centralized SDoC database would not cure. Whether a device properly qualifies for SDoC or an equipment-authorization exemption may depend on its technical characteristics, intended use, and compliance testing, information that a retailer or marketplace lacking physical access to the device ordinarily does not possess. A centralized database would establish only that information had been submitted; it would not establish that the device was properly classified or that the underlying compliance determination was correct. Creating such a database would also effectively impose the universal registration regime that INCOMPAS opposes for the reasons discussed in the preceding section. A targeted manufacturer-hosted record may make information supplied by the responsible party more accessible, but it should not convert a marketplace into an independent verifier of the device's authorization status. A responsible-party or seller attestation therefore should be sufficient unless the marketplace has actual knowledge that the information is materially false or fails to act after receiving sufficiently specific notice of a defect.

Even where database verification is possible, the Commission should not construe "reasonable steps" to require continuous or real-time product matching unless it first provides a reliable, scalable, machine-readable interface. The *Third R&O* acknowledges that the current

EAS tools have limitations affecting catalog-scale verification and directs Commission staff to address database access, application-programming interfaces, machine-readable data, rate limits, and related technical barriers.[95] Before imposing an automated verification obligation, the Commission should make the necessary interface operational, publish complete technical documentation, establish stable access rules, and provide a mechanism for notifying users of outages or changes to authorization status. A marketplace should not incur liability for an inability to complete a database check caused by Commission-system unavailability or access restrictions.

The Commission must define the "online point of sale" with sufficient precision to permit consistent implementation across different marketplace designs. It should confirm that the online point of sale is the product-listing page, the page on which the complete product specifications appear and from which a consumer can select "Add to Cart" or "Buy Now." Search advertisements, organic search results, shopping carts, and later checkout screens should not each trigger a separate obligation to duplicate the same information. A prominently displayed, clickable compliance badge or link to the applicable SDoC statement on the product-listing page should satisfy the display requirement. The *Third FNPRM* itself recognizes that placing a complete compliance statement in a product listing may consume substantial space and specifically asks whether a URL or QR code would provide a workable alternative.[96]

INCOMPAS also opposes requiring retailers and online marketplaces to obtain proof of a purchaser's FCC license and verify that information before completing a sale of equipment intended for licensed operators. Online marketplaces process transactions at scale and generally

---

[95] *Id.* paras. 59–60; see also *Third FNPRM* para. 216.

[96] *Third R&O* para. 66; *Third FNPRM* paras. 168, 215.

rely on product and purchaser information supplied by others. The *Third FNPRM* identifies no uniform mechanism for matching a particular device, license class, and purchaser across those transactions. Requiring verification before sale would therefore be technically infeasible for many retailers and online marketplaces and would impose substantial compliance burdens. The Commission should not adopt that requirement.[97]

The Commission should reject the suggestion that it expand marketplace liability or close the exemptions and should instead preserve the scope limitations it adopted for online display of FCC identifiers associated with certified equipment. The Commission grandfathered existing listings until they are substantively amended, excluded non-substantive automated changes from the definition of an update, and exempted listings for used devices and qualifying small sellers.[98] The same protections should apply to any SDoC-related requirement. Extending them would avoid the disproportionate cost of retrofitting existing catalogs and reduce barriers for occasional and small-business sellers without compromising enforcement against high-volume marketing of unauthorized or covered equipment.

Finally, the Commission should apply any new requirements prospectively and provide implementation time measured from the date on which all definitions, data fields, technical specifications, and necessary Commission interfaces are final and operational. Online marketplaces will need to modify seller-intake processes, revise contractual requirements, build validation and record-retention systems, and redesign product-listing interfaces across multiple shopping surfaces. The Commission should provide clear notice of an alleged deficiency and a

---

[97] *Third FNPRM* paras. 174–75.

[98] *Third FNPRM* para. 168; *Third R&O* paras. 71–73 & App. A (adopting 47 CFR § 2.803(c)(3)); see also 15 U.S.C. § 45f(f)(3) (defining "high-volume third-party seller" for purposes of the INFORM Consumers Act).

reasonable opportunity to correct it before initiating enforcement or requiring suppression of a lawful listing. These safeguards would preserve accountability while placing substantive compliance responsibility on the parties that control the information necessary to comply.

XII. ANY EXPEDITED REVOCATION PROCEDURE MUST PRESERVE NOTICE AND DUE PROCESS

The Commission proposes expanding its streamlined revocation procedures and allowing the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to revoke an equipment authorization after providing the grantee only ten days to respond.[99] INCOMPAS recognizes that expedited action may be appropriate where the Commission establishes material, willful misconduct or determines that public health, interest, or safety requires immediate action. The Commission should not, however, make an abbreviated process the default where the relevant facts, the existence of a violation, or the appropriate remedy remain disputed.

The Administrative Procedure Act generally requires written notice of the facts or conduct that may warrant revocation and an opportunity to demonstrate or achieve compliance, subject to limited exceptions for willfulness and circumstances involving public health, interest, or safety.[100] Consistent with those requirements, any notice should identify the specific authorization and conduct at issue and provide sufficient information for the grantee to respond meaningfully. Inadvertent or correctable errors should receive an opportunity to cure rather than result in automatic revocation.

---

[99] *Third FNPRM* paras. 182–86 & App. B (proposed 47 CFR § 2.939(c)–(d)).

[100] 5 U.S.C. § 558(c).

Ten days ordinarily will not provide sufficient time to investigate allegations involving technical testing, information supplied by laboratories or Telecommunication Certification Bodies, or records obtained through complex supply chains. The Commission should provide at least thirty days to respond, consistent with the period incorporated in its existing revocation procedures, unless the safety of life or property requires a shorter period.[101] Where material facts remain disputed, the Commission should preserve a meaningful opportunity for hearing and review and issue a written decision explaining the basis for any revocation.

XIII. THE COMMISSION SHOULD ADOPT NARROWER COVERED LIST OBLIGATIONS FOR SUBMARINE CABLES

INCOMPAS supports the Commission's proposal to limit the Covered List obligations applicable to submarine cable applicants and licensees to equipment and services covered by producer/provider-based determinations. A production location-based determination should apply in the submarine cable context only where the underlying determination specifically identifies national security threats involving submarine cable systems.[102] This approach would preserve the Commission's ability to address a location-based threat that actually implicates submarine cable infrastructure without automatically extending every production location-based entry to cable applicants and licensees.

The Commission adopted the relevant certifications and routine conditions in the *2025 Submarine Cable First Report and Order*. Those requirements generally prohibit applicants and licensees from using or adding equipment and services identified on the Covered List to the relevant submarine cable system, new segment, or landing point.[103] At the time, Covered List

---

[101] 47 CFR § 2.939(b); 47 U.S.C. § 312(c).

[102] *Third FNPRM* paras. 218, 220–22 & App. B (proposed 47 CFR §§ 1.70006(d), 1.70007(u)).

[103] *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in*

determinations identified equipment or services produced or provided by particular entities. The Commission subsequently added its first production location-based entries, including entries addressing foreign-produced UAS-related equipment and consumer routers.[104] Those determinations address risks associated with the identified product categories but do not necessarily implicate submarine cable infrastructure.

INCOMPAS therefore opposes automatically applying every production location-based determination to submarine cable systems. Doing so could impose restrictions based solely on where a product was produced even when the underlying national security determination neither considered nor identified a threat involving submarine cable facilities. It would also make the scope of cable applicants' and licensees' obligations turn on Covered List determinations developed for materially different products and operational environments. As the Commission recognizes, limiting the cable-specific requirements to producer/provider-based determinations while retaining production location-based determinations that specifically address submarine cable threats would "provide greater regulatory certainty and minimize burdens."[105]

This narrower approach would not diminish the security protections governing submarine cable infrastructure. Cable applicants and licensees remain subject to the certifications and routine conditions adopted in the *2025 Submarine Cable First Report and Order*, including cybersecurity and physical-security risk-management requirements. The Commission also has adopted restrictions on principal submarine cable equipment produced by entities owned by,

---

Sections 1.1102 through 1.1109 of the Commission's Rules, OI Docket No. 24-523, MD Docket No. 24-524, Report and Order and Further Notice of Proposed Rulemaking, 40 FCC Rcd 6481, 6540–48, paras. 105–22 & Appx. A (2025) (*2025 Submarine Cable First Report and Order*), corrected by Erratum, DOC-414544A1 (OIA and OMD Sept. 16, 2025), and Second Erratum, DOC-415107A1 (OIA and OMD Oct. 24, 2025).

[104] *Third FNPRM* para. 219.

[105] *Id.*

controlled by, or subject to the jurisdiction or direction of a foreign adversary.[106] These existing cable-specific protections address risks to submarine cable systems more directly than automatically applying a production location-based determination developed without reference to that infrastructure. Accordingly, INCOMPAS supports the Commission's proposal only to the extent that it narrows the Covered List obligations already imposed under sections 1.70006(d) and 1.70007(u) by excluding production location-based determinations that do not specifically identify national security threats involving submarine cable systems. INCOMPAS does not support any new or expanded obligation for submarine cable applicants or licensees.

XIV. THE COMMISSION SHOULD NOT ADOPT TERM LIMITS FOR EQUIPMENT AUTHORIZATIONS OR, AT MINIMUM, SHOULD LIMIT ANY SUCH TERMS TO COVERED EQUIPMENT

The *Third FNPRM* seeks comment on whether the Commission should impose prospective expiration dates on equipment authorizations, including whether a ten-year term would be appropriate and whether expiration should restrict the continued marketing or continued operation of previously authorized equipment.[107] Although the Commission states that "there may be significant value to the automatic expiration of an authorization," the does not identify evidence showing that the indefinite duration of equipment authorizations has caused a compliance failure or created a national-security gap.[108] The Commission should decline to impose term limits on the current record.

---

[106] *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6540-48, paras. 105–22 & App. A; *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 Through 1.1109 of the Commission's Rules*, OI Docket No. 24-523, MD Docket No. 24-524, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 26-42, at 31, para. 76 (June 30, 2026) (*2026 Submarine Cable Second Report and Order*); *Third FNPRM* at 219.

[107] See *Third FNPRM* paras. 208–10.

[108] *Id.* paras. 208–09.

Existing equipment certifications remain valid unless withdrawn, revoked, terminated, or affected by a subsequent change in the Commission's rules.[109] That framework permits the Commission to address equipment presenting an identified compliance or security concern without requiring every authorization holder to periodically renew an otherwise valid authorization. The passage of time alone does not alter the radiofrequency characteristics of an unchanged device or establish that the device has become noncompliant. Generalized concerns about equipment lifecycles do not justify converting all equipment authorizations into recurring licenses.

A uniform expiration requirement would impose substantial burdens without a corresponding demonstrated benefit. The *Third FNPRM* does not establish a renewal process, including whether renewal would be automatic or instead require a new application and additional technical submissions. It also leaves unclear how expiration would operate for equipment authorized through the Supplier's Declaration of Conformity process.[110] Manufacturers could consequently face rolling renewal obligations across large portfolios of unchanged products, with no certainty about the testing, documentation, or administrative review renewal would require.

These concerns are especially significant for network, enterprise, and data-center equipment used to support cloud services and artificial-intelligence infrastructure. INCOMPAS members report that such equipment may remain in productive use for seven to ten years or longer after authorization. A ten-year expiration period could therefore arrive while equipment remains actively deployed, supported, and compliant. Requiring reauthorization merely because

[109] *Id.* para. 208; 47 CFR § 2.939.

[110] See *Third FNPRM* paras. 209–10.

a fixed period has elapsed could disrupt the availability of replacement units and components for existing deployments without addressing a product-specific security concern.

On the present record, the Commission should not apply an equipment-authorization expiration date to the continued operation of equipment lawfully acquired while its authorization was valid. The *Third FNPRM* expressly asks whether expiration should apply to continued operation as well as continued marketing.[111] Applying expiration to continued operation could prevent consumers and businesses from using equipment they purchased and deployed in reliance on a valid authorization. For network and data-center operators, such a restriction could strand substantial investments and compel premature replacement of functioning, compliant equipment. The Commission has not identified evidence demonstrating that those consequences are necessary to address a defined national-security risk.

If the Commission nevertheless adopts term limits, it should confine them to covered equipment and to continued marketing after the applicable term expires. Expiration should not prohibit the continued operation of units lawfully marketed or acquired while the authorization remained valid. This distinction would permit any term limit to govern whether additional units may enter the market without retroactively disrupting equipment already purchased and deployed.

The Commission also should grandfather every equipment authorization issued before the effective date of any final rule establishing term limits. Applying a newly adopted expiration period to an existing authorization would unsettle reliance interests developed under the Commission's longstanding framework and could place equipment already in production or

[111] *Id.* para. 208.

deployment on an unanticipated renewal schedule. Grandfathering existing authorizations would ensure that any new term limit operates prospectively and does not alter the duration of authorizations granted under the rules in effect when the Commission issued them.

Accordingly, the Commission should decline to impose equipment-authorization term limits. If it nevertheless proceeds, any term should apply only to covered equipment authorized on or after the effective date of the new rule and govern only continued marketing after expiration rather than continued operation. This fallback does not reflect INCOMPAS support for term limits or for recurring renewal obligations applicable to equipment that is not covered.

XV. CONCLUSION.

For the foregoing reasons, INCOMPAS respectfully requests that the Commission adopt the recommendations set forth herein.

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 8, 2026