July 1, 2026

FCC FACT SHEET*

Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program

Third Report and Order and Third Further Notice of Proposed Rulemaking ET Docket No. 21-232

Background: The Third Report and Order would adopt rules that further strengthen the Commission's equipment authorization program against national security risks to the communications supply chain, building on the First and Second Report and Orders and the recent additions to the Covered List of uncrewed aircraft systems (UAS), UAS critical components, and routers produced in a foreign country. It would close the "component part loophole" by prohibiting the authorization of devices that incorporate logic-bearing hardware components produced by entities identified on the Covered List; clarify that the marketing rules reach online marketplaces and require those marketplaces to display the FCC ID at the online point of sale; require full certification for any modification or permissive change made by a Covered List entity; and adopt a definition of "critical infrastructure.". This will allow the Commission to safeguard U.S. communications networks and uphold the integrity of the equipment authorization process. The action is authorized pursuant to the Communications Act of 1934, the Secure and Trusted Communications Networks Act of 2019, and the Secure Equipment Act of 2021. The accompanying Third Further Notice of Proposed Rulemaking seeks comment on a series of further measures to close component-level and supply-chain loopholes, including bifurcating the Covered List into producer/provider-based and production location-based categories, enhancing supply-chain transparency through hardware and software bills of materials, restricting certain importation pathways for covered equipment, and strengthening post-market enforcement.

What the Third Report and Order Would Do:

- Closes the "component part loophole" by prohibiting the authorization of logic-bearing hardware components produced by entities identified on the Covered List, and of any device that incorporates such a component where the device would be prohibited had the Covered List entity produced the device itself.
- Clarifies that "marketing" includes online marketplaces that list, distribute, or offer unauthorized equipment, and requires online marketplaces to display the FCC ID of certified devices at the online point of sale.
- Requires full certification for any modification or permissive change made by an entity identified on the Covered List and bars such entities from using the Supplier's Declaration of Conformity (SDoC) process for any modification, whether to covered or non-covered equipment.
- Clarifies that previously-authorized equipment may not be modified so as to become covered equipment, and that "produced by" continues to be assessed under the totality of the circumstances.

*This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in ET Docket No. 21-232 which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs). Before filing, participants should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 *et seq*.

- Adopts a narrowed definition of "critical infrastructure"—the USA PATRIOT Act § 1016(e) definition, guided by the 16 critical infrastructure sectors and 55 National Critical Functions—removing the "connected to" language the D.C. Circuit found overbroad.
- Corrects a cross-reference error in section 2.903 and related administrative errors in section 2.1204 of the rules.

What the Third Further Notice of Proposed Rulemaking Would Do:

- Proposes to bifurcate the Covered List into producer/provider-based and production location-based categories, with a conforming reorganization of the Part 2 rules and a two-column Covered List website.
- Seeks comment on supply-chain transparency measures, including hardware and software bills of materials (HBOM/SBOM) and component-origin reporting, codifying a definition of "produced by," and curbing white-labeling and "electrically identical" device abuse.
- Proposes broader component prohibitions—prohibiting, or presuming against, authorization of devices incorporating any hardware component, software, or firmware produced by a Covered List entity—and requiring certification for all devices in Covered List sectors (UAS, UAS critical components, and routers).
- Proposes to tighten covered equipment controls across importation (§ 2.1204), marketing (§ 2.803), pre-authorization operation (§ 2.805), and use of the FCC logo (§ 2.1074).
- Seeks comment on strengthening enforcement through streamlined revocation (§ 2.939), term limits on equipment authorizations, registration of SDoC devices, and a U.S.-based liable party requirement for FCC-certified equipment.
- Proposes to codify and make permanent the waivers permitting software and firmware (and limited hardware) updates that mitigate consumer harm for already-authorized covered equipment.
- Proposes to codify Covered List definitions ("produced in a foreign country," "UAS critical components," and "routers"), modernize the EAS database and data-analytics capability, and tailor submarine-cable Covered List certifications to producer/provider-based determinations.

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

THIRD REPORT AND ORDER AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING*

Adopted: [ ] **Released: [ ]**

Comment Date: [30 days after date of publication in the Federal Register]
Reply Comment Date: [45 days after date of publication in the Federal Register]

By the Commission:

TABLE OF CONTENTS

* This document has been circulated for tentative consideration by the Commission at its July 22, 2026 open meeting. The issues referenced in this document and the Commission's ultimate resolutions of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The Commission's ex parte rules apply and presentations are subject to "permit-but-disclose" ex parte rules. See, e.g., 47 CFR §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. See 47 CFR §§ 1.1200(a), 1.1203.

I. INTRODUCTION

1. In this *Third Report and Order*, we take further steps to strengthen the Commission's equipment authorization program against national security risks to the communications supply chain, building on the *First Report and Order*,[1] the *Second Report and Order*,[2] and the recent updates to the Covered List addressing uncrewed aircraft systems (UAS), UAS critical components, and routers produced in a foreign country.[3]

2. The *Third Report and Order* closes the component part loophole by prohibiting authorization of devices incorporating logic-bearing hardware components if—had the entity produced the device itself—it would be prohibited from authorization. It further requires that any modification or permissive changes by entities identified on the Covered List undergo full certification and clarifies that the marketing rules reach any entity—including ecommerce platforms—that market unauthorized equipment. The *Third Report and Order* also requires such platforms to provide an FCC ID at the online point of sale. Finally, it amends our definition of "critical infrastructure," as used on the Covered List.

3. The accompanying *Third Further Notice of Proposed Rulemaking* invites comment on a

[1] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232 and EA Docket 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking, 37 FCC Rcd 13493 (2022) (First Report and Order).

[2] *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 (2025) (Second Report and Order).

[3] Press Release, FCC, FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models (Mar. 23, 2026), https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf; Press Release, FCC, Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List (Dec. 22, 2025), https://docs.fcc.gov/public/attachments/DA-25-1086A1.pdf.

series of further measures, to include: bifurcating the Covered List into producer/provider-based and production location-based categories; enhancing supply chain transparency through software bill of materials (SBOM) and hardware bill of material (HBOM) disclosures; restricting certain importation pathways for covered equipment; strengthening post-market enforcement, including streamlined revocation procedures, term-limited equipment authorizations, and a U.S.-based liable party requirement; and requiring registration of equipment authorized through the Supplier's Declaration of Conformity (SDoC) process.

II. BACKGROUND

A. The First Report and Order and Further Notice

4. Pursuant to the Secure and Trusted Communications Networks Act ("Secure Networks Act"), the Commission publishes the Covered List, a list of equipment and services that have been specifically determined by enumerated sources to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[4] In June 2021, the FCC opened this proceeding and issued a Notice of Proposed Rulemaking ("NPRM") that proposed banning the authorization of equipment on the Covered List. In November 2021, while this proceeding was pending, Congress enacted the Secure Equipment Act of 2021, which identified this proceeding by docket number and directed the Commission to adopt rules prohibiting authorization of covered equipment.[5]

5. In 2022, the Commission issued the *First Report and Order.* As mandated by Congress in the Secure Equipment Act, the Commission adopted rules to ban authorizations of covered equipment.[6] The rules explicitly prohibited authorization of covered equipment through the FCC's certification and SDoC procedures.[7] The rules reformed the certification process by requiring any applicant for certification to attest that the equipment at issue was *not* covered equipment, attest to its status as an entity identified on the Covered List (including subsidiaries and affiliates), and designate a U.S.-based agent for service of process.[8] The *First Report and Order* made clear that equipment without an authorization due to its being on the Covered List could not be imported or marketed and could not avail itself of exemptions from equipment authorization requirements.[9] It also adopted streamlined revocation procedures for authorized equipment for which an applicant submitted false attestations regarding the covered status of equipment.[10] The *First Report and Order* identified as covered equipment subject to prohibition all telecommunications and video surveillance equipment produced by Huawei and ZTE (and subsidiaries and affiliates thereof), and all telecommunications and video surveillance equipment by Hikvision, Dahua, and Hytera to the extent that such equipment is used for "the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, or other national security purposes."[11] The *First Report and Order* also clarified that equipment on the Covered List included equipment produced by subsidiaries and affiliates of named entities.[12] The Commission also

[4] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609 (Secure Networks Act); 47 CFR §§ 1.50002, 1.50003.

[5] Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (codified at 47 U.S.C. § 1601 note), *available at* https://www.congress.gov/bill/117th-congress/house-bill/3919/text.

[6] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program,* ET Docket No. 21-232, Report and Order, Order, and Further Notice of Proposed Rulemaking, 37 FCC Rcd 13493, 13514 (2022) (*First Report and Order*).

[7] 47 CFR §§ 2.903, 2.906(d).

[8] 47 CFR §§ 2.911(d)(5)-(7).

[9] *First Report and Order,* 37 FCC Rcd at 13529-30, paras. 87-91.

[10] *Id.* at 13535-37, paras. 108-113.

[11] *Id.* at 13561-64, paras. 176-181.

[12] *Id.* at 13564-67, paras. 182-186.

adopted the *First Further Notice* seeking comment on proposals to expand the scope of prohibitions to include component parts, revoke existing equipment authorizations of covered equipment, and to impose greater accountability under U.S. law on foreign-based grantees of equipment certifications.[13]

6. Hikvision USA, Inc. and Dahua Technology USA, Inc. thereafter appealed certain aspects of the *First Report and Order* to the U.S. Court of Appeals for the District of Columbia Circuit, which issued a partial remand.[14] Specifically, the court vacated one portion of the Commission's decision defining "critical infrastructure" for purposes of understanding when video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua is used "for the purpose of … physical security surveillance of critical infrastructure," statutory language drawn from Congress's proscription regarding such equipment as set forth in section 889(f)(3) of the National Defense Authorization Act of 2019 (NDAA).[15] The court found that the Commission's definition of "critical infrastructure" was "unjustifiably broad," and remanded those portions of the *Equipment Authorization Security R&O* to the Commission to "comport its definition and justification for it" with the NDAA statutory provision.[16]

B. The Second Report and Order and Second Further Notice

7. In October 2025, the Commission adopted the *Second Report and Order* to strengthen the FCC's equipment authorization program by closing loopholes that previously allowed devices or components that pose national security risk to enter the U.S. market.[17] The *Second Report and Order* clarified that covered equipment includes modular transmitters, and it prohibited authorization of any device containing a modular transmitter that is itself covered equipment.[18] It also established a new process to limit existing equipment authorizations by blocking further importation and marketing of already authorized- covered equipment while allowing continued use, and it clarified key statutory terms such as "produced by" to ensure entities cannot evade Covered List restrictions through rebranding or partial manufacturing.[19] The Order further barred modifications or permissive changes to covered equipment or previously authorized equipment that would become covered as a result of the modification or permissive change.[20]

8. The *Second Further Notice* sought comment on additional measures to fortify the program, including whether to prohibit authorization of equipment containing other components, including any equipment that includes logic-bearing hardware components;[21] a refined definition of "critical infrastructure" following the D.C. Circuit remand;[22] and whether any modification made by an entity identified on the Covered List should always require full certification.[23] The *Second Further Notice* also proposed expanded enforcement tools, such as clarifying what constitutes "marketing,"

[13] *Id.* at 13599-616, paras. 267-326.

[14] *See generally Hikvision USA, Inc. v. Federal Communications Commission*, 97 F.4th 938 (D.C. Cir. 2024) (*Hikvision*).

[15] *Hikvision*, 97 F.4th at 948-50. *See* Pub. L. 115-232, § 889, 132 Stat. 1636, 1917-19 (2018) (2019 NDAA § 889).

[16] *Hikvision*, 97 F.4th at 950.

[17] *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 (2025) (*Second Report and Order*).

[18] *Id.* at 8436-46, paras. 14-31.

[19] *Id.* at 8447-58, paras. 32-53.

[20] *Id.* at 8447, paras. 54-55.

[21] *Id*. at 8459, paras. 58-66

[22] *Id.* at 8463-68, paras. 68-80.

[23] *Id.* at 8468-69, paras. 81-83.

strengthening accountability across importers and distributors, and requiring online display of FCC IDs and periodic verification of authorization status to prevent unauthorized devices from entering or remaining in U.S. commerce.[24]

C. Covered List additions of equipment "produced in a foreign country"

9. Starting in December 2025, the Commission's Public Safety and Homeland Security Bureau (PSHSB)—following specific determinations pursuant to the Secure Networks Act—updated the Covered List several times to identify categories of equipment produced in a foreign country. These updates were the first instances of covered equipment and services being defined according to the production location of a class or sector of products and services, rather than in terms of the producer or provider of the equipment or services. These determinations included all UAS, UAS critical components, and routers produced in a foreign country, subject to certain carveouts. We refer to these determinations as production location-based determinations, as opposed to the producer/provider-based determinations that comprise the rest of the Covered List.

10. In December 2025, PSHSB made a two-part update to the Covered List in response to a national security determination made by an Executive Branch interagency body. First, PSHSB added all UAS and UAS critical components produced in a foreign country to the Covered List.[25] This was the first production location-based determination added to the Covered List, as opposed to producer/provider-based determinations that comprised the rest of the Covered List. Second, it added all communications and video surveillance equipment "listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act" based on a more traditional producer/provider-based determination identifying the producers of communications and video surveillance equipment as included in the Executive Branch national security determination.[26] In January 2026, in response to further determinations by the Department of War (DoW), PSHSB removed certain UAS and UAS critical components from the Covered List temporarily through January 2027; the removals applied to equipment on the Defense Contract Management Agency's (DCMA) Blue UAS Cleared List and to equipment qualifying as "domestic end products" under the Buy American standard.[27] PSHSB later removed specific models of covered UAS and UAS critical components from the Covered List pursuant to Conditional Approvals granted by DoW for limited time periods.[28]

11. In March 2026, PSHSB added the second production location-based determination to the Covered List for "routers produced in a foreign country, except routers which have been granted a

[24] *Id.* at 8469-72, paras. 84-93.

[25] *Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed In Section 1709 of the FY2025 NDAA, to FCC Covered List*, WC Docket No. 18-89, Public Notice, DA 25-1086 (Dec. 22, 2025) (*First UAS Public Notice*).

[26] *Id.* (citing Pub. L. 118-159).

[27] *Public Safety and Homeland Security Bureau Announces Exemption of Certain Uncrewed Aircraft Systems (UAS) and UAS Critical Components from FCC Covered List*, WC Docket No. 18-89, Public Notice, DA 26-22 (Jan. 7, 2026) (*Second UAS Public Notice*).

[28] *See, e.g.*, *Public Safety and Homeland Security Bureau Announces Conditional Approval of Certain Uncrewed Aircraft Systems (UAS) and UAS Critical Components and Exemption from FCC Covered List*, WC Docket No. 18-89, Public Notice, DA 26-253 (Mar. 18, 2026) (SiFly Aviation, Mobilicom SkyHopper, ScoutDI, Verge Aero); *FCC's Public Safety and Homeland Security Bureau Announces Conditional Approval of Certain Routers and Uncrewed Aircraft Systems (UAS) and Exemption from FCC Covered List* (Apr. 14, 2026) (sees.ai v. USA). For a full list of the conditional approvals, *see* Federal Communications Commission, https://www.fcc.gov/supplychain/coveredlist#conditional-approvals (last visited June 26, 2026).

Conditional Approval by DoW or DHS."[29] It later removed specific models of covered routers from the Covered List pursuant to Conditional Approvals granted by DoW for limited time periods.[30]

12. In response to the UAS and router class-based determinations, OET waived rules the Commission had adopted in the *Second Report and Order* that would have prohibited permissive changes to previously-authorized equipment, such as software and firmware security updates.[31] Without these waivers, previously-authorized UAS, UAS critical components, and routers produced in a foreign country would have become prohibited covered equipment after such permissive change under the rules adopted in the *Second Report and Order.* These waivers, which now expire in 2029, currently allow such previously-authorized UAS, UAS critical components, and routers to continue to receive software and firmware security updates to mitigate harm to U.S. consumers.[32] Since May 2026, in response to petitions for waivers, OET has waived rules for one year to allow limited permissive hardware changes to previously-authorized consumer-grade routers to address unavoidable supply-chain shortages and the public interest need to prevent disruptions in the availability of broadband for customers.[33]

III. THIRD REPORT AND ORDER

13. In this *Third Report and Order*, we adopt rules that further strengthen the Commission's equipment authorization program against national-security threats to the communications supply chain. First, we close the component part loophole to our Covered List rules. We find that devices containing logic-bearing hardware components produced by an entity identified on the Covered List pose similar unacceptable risks as covered equipment itself. Therefore, we prohibit the authorization of logic-bearing hardware components produced by Covered List entities and devices containing such logic-bearing hardware components if—had the device itself been produced by the Covered List entity—the device would be prohibited. Second, we clarify that the term "marketing" includes the activities engaged in by online marketplaces that list, distribute, or offer for sale equipment produced by third-party sellers, and we require online marketplaces to display the FCC ID of certified devices at the online point of sale.[34]

---

[29] *FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List,* WC Docket No. 18-89, Public Notice, DA 26-278 (Mar. 23, 2026).

[30] *See, e.g.*, *FCC's Public Safety and Homeland Security Bureau Announces Conditional Approval of Certain Routers and Uncrewed Aircraft Systems (UAS) and Exemption from FCC Covered List,* WC Docket No. 18-89, Public Notice, DA 26-351 (Apr. 14, 2026) (Netgear and Adtran routers); *FCC's Public Safety and Homeland Security Bureau Announces Conditional Approval of Certain Routers and Exemption from FCC Covered List,* WC Docket No. 18-89, Public Notice, DA 26-390 (Apr. 22, 2026) (Amazon and eero routers). Federal Communications Commission, https://www.fcc.gov/supplychain/coveredlist#conditional-approvals (last visited June 26, 2026).

[31] *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered UAS and UAS Critical Components,* ET Docket No. 21-232, Public Notice, DA 26-69 (Jan. 21, 2026); *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered Routers,* ET Docket No. 21-232, Public Notice, DA 26-286 (Mar. 23, 2026).

[32] *Office of Engineering and Technology Announces Extension and Expansion of Waiver of Prohibitions on Certain Software and Firmware Permissive Changes to Certain Covered UAS, UAS Critical Components, and Routers,* ET Docket No. 21-232, Public Notice, DA 26-454 (May 8, 2026).

[33] *See, e.g., In the Matter of AT&T Services, Inc.,* ET Docket No. 21-232, Order, DA 26-491 (May 15, 2026); *In the Matter of NCTA - The Internet & Television Association Petition for Expedited Waiver to Permit Targeted Class I and Class II Permissive Hardware Changes to Covered Routers*, ET Docket No. 21-232, Order, DA 26-571 (rel. June 9, 2026) (NCTA Waiver Order); *In the Matter of Sercomm Corporation; Petition for Expedited Waiver of Sections 2.932(b) and 2.1043(b) of the Commission's Rules to Permit Targeted Class I and Class II Permissive Hardware Changes to Covered Routers*, ET Docket No. 21-232, Order, DA 26-572 (rel. June 9, 2026).

[34] We recognize that Congress defined the term "online marketplace" in the Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act (INFORM Consumers Act), 15 U.S.C. § 45f(f)(4), a statute administered by the Federal Trade Commission. We adopt that definition here, but we do so as an independent exercise of our own authority under sections 4(i), 302(a), and 303 of the Communications Act of 1934, as amended, (continued….)

Third, we clarify that previously authorized equipment may not be modified in a manner that would render it covered equipment and that the term "produced by" continues to be evaluated under the totality of the circumstances. Fourth, we require that any modification or permissive change made by an entity identified on the Covered List undergo full certification, and we clarify that no such entity may rely on the SDoC process for any modification, whether to covered or non-covered equipment. We also adopt a definition of "critical infrastructure" as used in the Covered List context. Finally, we correct a cross-reference error in section 2.903 of our rules.

A. Logic-Bearing Hardware Components.

14. In the *Second Report and Order*, the Commission adopted rules extending its ban on authorizing covered equipment to also ban authorizing any device that contains a modular transmitter that is itself covered equipment.[35] The *Second Further Notice* sought comment on whether this prohibition should extend to other component parts that, if included in another device, would cause the device to pose similar unacceptable risks to the national security of the United States or the safety and security of U.S. persons as other equipment on the Covered List.[36] We further requested comment on which components produced by entities identified on the Covered List, should trigger authorization bans, how to identify such components with sufficient specificity, and the feasibility and cost of requiring detailed component reporting. The Commission specifically sought comment on whether the Commission "should … prohibit authorization of equipment that includes component parts that are logic-bearing hardware, firmware, or software produced by entities identified on the Covered List."[37] This terminology was based on a Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom) filing in another proceeding, which noted that national security concerns arise from "firms using logic-bearing hardware, firmware, or software … from high-risk providers identified by the United States government."[38]

15. The Commission also sought comment on broader proposals such as prohibiting equipment containing logic-bearing hardware components that are produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, regardless of whether they are identified on the Covered List.[39] This was an approach suggested by the Hudson Institute, which cited risks if devices contained such components produced by Covered List entities and/or entities owned by,

---

47 U.S.C. §§ 154(i), 302a, 303, and the Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423, and not in reliance on 15 U.S.C. § 45f, which confers no authority on this Commission. We find that aligning our terminology with the INFORM Consumers Act's established definition serves the public interest by promoting regulatory consistency and reducing compliance burdens for the online marketplaces already subject to that definition under the FTC's regime, while we retain the discretion to depart from that definition where the purposes of our equipment authorization program so require.

[35] *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, FCC 25-71 (Second Report and Order),* paras. 14-31.

[36] *Id* at 8459, para. 59.

[37] *Id* at 8459, para. 59.

[38] *Id* at 8459, para. 59, n. 216 (citing *Review of International § 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Risks,* IB 23-119, MB 23-134 at 6 (Aug. 31, 2023), https://www.fcc.gov/ecfs/document/10831697221812/2 (Team Telecom comment)). Team Telecom often advises the Commission on national security threats from foreign involvement in the U.S. communications sector. *See generally*, Executive Order 13913, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," (Apr. 4, 2020), https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states; https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf.

[39] *Id* at 8459, para. 64.

controlled by, or subject to the jurisdiction.[40] The Commission also asked for comments on appropriate transition periods and their impact on supply chains. Finally, the Commission sought comment on expanding security investigations, or creating partnerships or trusted supplier programs, all while balancing national security protections with minimizing unnecessary market disruption.

16. We find that—from a technical perspective—devices incorporating logic-bearing hardware components produced by Covered List entities pose essentially the same unacceptable risks to the national security of the United States or the safety and security of United States persons as if the device itself were produced by that Covered List entity. We therefore prohibit authorization of devices incorporating such logic-bearing hardware components if—had the Covered List entity produced the device itself, rather than just a component—the device would be prohibited from receiving authorization.

17. Some examples of the rules we adopt today include:

- Example (1) Under our current rules, if "Device X produced by Entity A" were on the Covered List, the Commission would cease authorizing any Device X produced by Entity A. We now adopt rules to prohibit the authorization of Device X incorporating an Entity A-produced logic-bearing hardware component, no matter who produced the rest of Device X.
- Example (2) If "Service Y provided by Entity B" were on the Covered List, this would have no effect on the equipment authorization process under our current rules or the rules we adopt today.
- Example (3) Under our current rules, if "Device Z produced by Entity C to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes" were on the Covered List, the Commission would cease authorizing any Device Z produced by Entity C until Entity C submits—and gets approved—an FCC compliance plan. After this, Entity C could get its devices authorized for non-covered use cases.[41] Under the rules we adopt today, the Commission would similarly cease authorizing any Device Z incorporating an Entity C-produced logic-bearing hardware component, no matter who produced the rest of Device Z, similarly contingent on approval of Entity C's compliance plan. After such approval, the Commission would authorize a Device Z incorporating an Entity C-produced logic-bearing hardware components for non-covered purposes.

18. Prohibiting the authorization of such devices is generally consistent with the Secure Networks Act and the Secure Equipment Act,[42] because it aims to prevent the same harm that Congress addressed in those Acts—the importation of devices the security of which has been compromised by Covered List entities. Indeed, where a Covered List entity has produced an important component of equipment, that equipment can pose essentially the same risks that Congress was seeking to address when it directed the Commission to prohibit authorizing covered equipment in the Secure Equipment Act. And

[40] *See* Hudson *ex parte* in *Second Report & Order and Further Notice of Proposed Rulemaking* at 1-2.

[41] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, ET Docket No. 21-232 and EA Docket 21-233, Report and Order and Further Notice of Proposed Rulemaking, 37 FCC Rcd 13493 (2022) (EA Security R&O and FNPRM),* para. 180 ("Before any … 'telecommunication equipment' or 'video surveillance equipment'" produced by entities whose equipment is subject to a use-based Covered List entry "will be authorized for market or sale, the applicant seeking approval of any 'covered' equipment produced by any of these entities (or their subsidiaries or affiliates) must submit a specific plan associated with the equipment, which will be reviewed by the full Commission and only approved if the measures that are and will be taken are sufficient to prevent the marketing and sale of such equipment for purposes prohibited under section 889(f)(3)(B) of the 2019 NDAA.)

[42] It is also consistent with the Commission's modular transmitter rules adopted last year in the *Second EA Security R&O*.

logic-bearing hardware components, when produced by Covered List entities whose equipment has been determined to pose unacceptable national security or public safety risks, and included within a device, can, in addition to other threats, enable these entities to "access, store, disrupt, and/or misroute U.S. communications," unbeknownst to the user,[43] representing a national security risk.

19. We have independent authority for this action under the Communications Act. Section 302a of the Communications Act authorizes the Commission to regulate radio frequency devices "consistent with the public interest, convenience, and necessity."[44] It is well established that the public interest standard permits consideration of national security risks.[45] Moreover, Section 303(g) directs the Commission—again, "as public convenience, interest, or necessity requires"—to "generally encourage the larger and more effective use of radio in the public interest."[46] Section 303(r) confers associated rulemaking authority to "[m]ake such rules and regulations and prescribe such restrictions and conditions . . . as may be necessary to carry out" the Commission's assigned mission and responsibilities.[47] And Section 303(e) specifies that the Commission may "[r]egulate the kind of apparatus to be used" not only as to "the purity and sharpness of the emissions" but also as to "external effects" more broadly,[48] a phrase that readily encompasses national security-related effects. Taking account of this authority, we find that an "effective" use of radio spectrum includes guarding against radiofrequency devices that have been deemed to pose an unacceptable threat to the national security of the United States (or that, in the case of the logic-bearing hardware components and devices here, would be the subject of a Covered List determination had the device itself been produced by the Covered List entity). Prohibiting the authorization of such devices likewise serves "the purpose of the national defense" and "the purpose of promoting safety of life and property."[49]

20. Given the lack of support in the current record, we do not adopt broader proposals to ban equipment authorizations for equipment incorporating components where there is not a nexus to a specific national security determination resulting in additions to the Covered List. We do not, at this time, adopt proposals to ban components produced by any person controlled by or subject to the jurisdiction or direction of a foreign adversary, but we reserve the right to act in response to the record on this point in a future Report and Order in this proceeding.

21. We further find that devices incorporating logic-bearing hardware components produced by Covered List entities pose the same or substantially similar "unacceptable risks" as devices produced

[43] *China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order on Revocation and Termination, 36 FCC Rcd 15966, 15967, para. 2 (2021), *aff'd*, *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2022).

[44] 47 U.S.C. § 302a(a).

[45] *See, e.g., Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421, 439-40, 443-44 (5th Cir. 2021); *China Telecom (Ams.) v. FCC*, 57 F.4th 256, 261-62 (D.C. Cir. 2022); *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1164-65 (D.C. Cir. 2023); *China Unicom (Ams.) Ops. Ltd. v. FCC*, 124 F.4th 1128, 1135, 1150, 1151-54 (9th Cir. 2024).

[46] 47 U.S.C. § 303(g).

[47] *Id.* § 303(r); *see also id.* § 154(i).

[48] *Id.* § 303(e).

[49] 47 U.S.C. § 151; see *Huawei*, 2 F.4th at 439; *Pac. Networks*, 77 F.4th at 1164-65. The Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994), buttresses our authority under the Communications Act. Section 105 of CALEA requires that telecommunications carriers "ensure that any interception of communications access or access to call-identifying information . . . can be activated only in accordance with a court order or other lawful authorization." 47 U.S.C. § 1004. And Section 301 directs the Commission to prescribe implementing rules "to require appropriate authorization to activate interception of communications" and "to prevent any such interception or access without such authorization." 47 U.S.C. § 229(a)-(b). Our equipment authorization rules, including the rule we adopt today, bear on carriers' ability to meet their obligations under Section 105 by preventing authorization of equipment that could be connected to the carriers' networks.

by the Covered List entities themselves. Therefore, if the Commission prohibits the authorization of certain equipment produced by Covered List entities, the Commission should similarly prohibit authorization of any equipment that contains Covered List entity-produced logic-bearing hardware components, whether by SDoC or by certification.

22. Several commenters supported adopting related prohibitions. David Feith and Michael Sobolik, scholars at the Hudson Institute who filed in last year's proceeding (Feith & Sobolik), expressly supported expanding restrictions to cover "risks posed by equipment containing logic-bearing components produced by Covered List entities."[50] They note that logic-bearing hardware components, such as semiconductors, IoT modules, optical transceivers, and printed circuit boards, among other components can be exploited and argue that without such a restriction, Americans and American critical infrastructure would be "vulnerable to remote access, data collection, and exploitation."[51] Chris McGuire similarly urges us to "prohibit authorization of any device that contains logic-bearing hardware—semiconductors, IoT and cellular modules, optical transceivers, baseband processors, and similar programmable components—produced by any entity on the Covered List."[52] He notes that "[a] compromised semiconductor can subvert the entire device in which it is installed," and that "[t]he national security risk posed by a Huawei chip embedded inside a device is the same risk posed by a Huawei device."[53] Finally, he notes that Covered List entities are active in producing logic-bearing hardware components, making this risk manifest.[54] He urges us to go further by applying the prohibition not just to logic-bearing hardware, but also to logic-bearing software and firmware.[55] The Foundation for Defense of Democracies (FDD) urges us to go further yet and generally supports prohibiting the authorization of any device containing any component produced by Covered List entities and so necessarily supports this prohibition.[56] Commenter Somos supports applying a prohibition on wireless chipsets, trust platform modules, cryptographic elements, and other connectivity-enabling components, which are all representative examples of logic-bearing hardware components, because these components directly impact the risk profile of the complete product.[57] Such components are quintessential examples of logic-bearing hardware (though of course not exhaustive).

23. We prohibit authorization of devices that incorporate logic-bearing hardware components produced by an entity identified on the Covered List if—had the entity produced the device itself, rather than just a component—the device would be prohibited from receiving authorization under our current rules. We agree with Team Telecom's earlier comment that "foreign adversary influence on U.S. communications networks" can flow from firms using "logic-bearing hardware…from high-risk providers identified by the United States government," such as entities identified on the Covered List.[58] Although this comment was made in a different proceeding, as we often do, we defer to Team Telecom's expertise

[50] Feith & Sobolik Comment at 1.

[51] Feith & Sobolik Comment at 2.

[52] Chris McGuire Comment at 2.

[53] *Id.*

[54] Chris McGuire Comment at 3-5.

[55] Chris McGuire Comment at 2.

[56] FDD comments at 1-2.

[57] Somos Comment at 3.

[58] *Review of International § 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Risks,* IB 23-119, MB 23-134 at 6 (Aug. 31, 2023), https://www.fcc.gov/ecfs/document/10831697221812/2 (Team Telecom comment)

in identifying national security risks.[59]

24. We also base our rule today on our own independent expert judgment as to how a device with a compromised logic-bearing hardware component can undermine the security of an entire device. The principal that "trust starts in silicon" reflects the widely recognized role that hardware plays as a foundational element of system security upon which software protections depend.[60] From a technical perspective, communications equipment containing a logic-bearing hardware component produced by a Covered List entity may present supply-chain and cybersecurity risks comparable to those posed by covered communications equipment that as a whole is produced by a Covered List entity. A Covered List entity that produces a semiconductor, for example, incorporated into communications equipment could potentially introduce malicious logic, firmware, hidden functionality or other compromised features into such components. Depending on the component's function, privileges, and integration into the device, such functionality may enable the interception, recording, modification, rerouting, or exfiltration of sensitive information. Compromised logic-bearing hardware components may also facilitate sabotage, unauthorized access, or other malicious activity regardless of their visibility to end users or the branding of the final product. In addition, supply chains controlled by Covered List entities may provide opportunities for persistent access, influence, or exploitation throughout the lifecycle of a device.

25. These concerns are consistent with guidance from the National Institute of Standards and Technology (NIST), which recommends maintaining visibility into logic-bearing hardware components as part of a cybersecurity supply chain risk management program, including through the use of bills of materials that identify such components.[61] Certain logic-bearing hardware components can serve as, or materially affect, the root of trust because they operate at foundational layers of computing. Where a security-critical hardware component is compromised, software-based security controls and encryption may be substantially undermined. Moreover, standard cybersecurity defenses including antivirus software, firewalls, and Endpoint Detection and Response (EDR) tools are generally not designed to detect malicious logic or hardware-level backdoors embedded directly into silicon. Unlike many software vulnerabilities, which can often be patched or otherwise remediated, malicious modifications at the hardware level in logic-bearing hardware components may persist throughout a device's lifecycle and can be exceptionally difficult to detect, analyze, or remediate.

26. Besides Team Telecom's earlier comment, several other commenters in this proceeding support our decision. As Chris McGuire notes, logic-bearing hardware components are not passive; each "executes its own firmware beneath the device's operating system, the most privileged layer of the system. A compromise at this layer is more powerful, more persistent, and harder to detect than a compromise at the application layer."[62] McGuire also identifies numerous security reports demonstrating the possibility of compromise at the logic-bearing hardware component layer—down to the chip level.[63] Most important for this rule, we agree with McGuire that "the party that compromises a chip need not be the company that assembles the finished device" as "[a] single actor anywhere in the design or fabrication chain can introduce the defect."[64] We also agree with Feith & Sobolik that logic-bearing hardware components, electronic parts that process, store, and transmit data…can be embedded invisibly within

[59] *See, 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 and MD Docket No. 24-524, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-82 (rel. Aug. 26, 2024), para. 145.

[60] *See* E. Levine, *The Die is Cast,* ACM Queue (Jan. 2021), https://cacm.acm.org/practice/the-die-is-cast/

[61] NIST SP 800-161 at p. 224, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf (May 2022).

[62] Chris McGuire Comment at 2.

[63] Chris McGuire Comment at 2-3.

[64] Chris McGuire Comment at 3.

larger systems, leaving end users unaware of their provenance even as they enable potential avenues of espionage or disruption."[65]

27. Somos does not specifically address logic-bearing hardware components, but Somos does advocate for component-based prohibitions on a sample of components that are representative of logic-bearing hardware components, namely, "communications modules, wireless chipsets, trust platform modules ("TPMs"), cryptographic elements, and other connectivity-enabling components."[66] We believe that "connectivity-enabling components" is well-captured by our term "logic-bearing hardware components," because logic is embedded into the function of each these components.[67] Communications modules require logic to process signals – to packetize, buffer, and arbitrate communications. Wireless chipsets (Wi-Fi, Bluetooth, cellular) contain embedded processors and protocol stacks; they require logic to make decisions about frequency, power, and retransmission. TPMs and cryptographic elements require logic because they provide entirely computational functions – such as key generation, signing, verification, entropy management. Platform modules, such as baseboard management controllers and platform controllers, govern other controllers and require logic to do so. These connectivity enabling components interpret signals and translate between protocols using logic. We agree with Somos that such components are "integral to a device's overall cybersecurity posture."[68] They contain logic that can carry firmware, keys, or hidden vulnerabilities or hardware-level backdoors. We further agree that, "[b]ecause these components govern the transmission, security, and trust relationships of data moving into or out of a device, their integrity directly affects the risk profile of the complete product."[69] Furthermore, we agree with FDD that adopting a broad prohibition is important, because in general, the Commission "should enact the broadest possible prohibitions" when it comes to foreign component parts, "to safeguard U.S. national security."[70]

28. We are mindful of several commenters who cautioned that the term "logic-bearing hardware" is vague and ill-defined.[71] For example, CTIA states that "logic-bearing hardware" "is simply not specific enough to allow affected parties to identify the equipment that would be prohibited from authorization."[72] Other commenters urge the Commission to codify "bright line rules clearly identifying components that are covered."[73] While we do not adopt a component-by-component approach, we do codify a detailed definition, to guide companies within the communications industry. We define logic-bearing hardware components to be any device, system, module, sub-assembly, integrated circuit, or other physical component that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques; inclusive of telephone equipment that uses digital techniques or any device, system, module, sub-assembly, integrated circuit, or other physical component that generates and uses radio frequency energy for the purpose of performing data processing

[65] David Feith and Michael Sobolik Comment at 1 (paraphrased). Feith & Sobolik further highlight that "[t]hese risks are particularly pronounced with data centers," where logic-bearing hardware components pose acute risks. *Id*. at 2.

[66] Somos Comment at 3.

[67] Somos also refers at one point to "any device incorporating components manufactured by entities on the Covered List," which further suggests that Somos has a broad view of which components should be subject to the prohibition, rather than a specific subset of named components. *See* Somos Comment at 3.

[68] Somos Comment at 3.

[69] *Id*.

[70] FDD Comment at 1-2.

[71] CTIA Comment at 14; CTA Comment at 6 ("[U]nclear component restrictions could slow product development cycles, increase manufacturing costs, and limit design options."); *See also* ITI Comment at 4 (arguing that "[b]road categories like… 'logic-bearing hardware,' …are overbroad and unworkable.").

[72] CTIA Comment at 14.

[73] Garmin Comment at 5.

functions, such as electronic computations, operations, transformations, recording, filing, sorting, storage, retrieval, or transfer. This definition provides a clear definition using language from our existing definition of "digital device" under section 15.3(k) of our rule. The only substantial distinction between our definition and the longstanding digital device definition is that the logic-bearing hardware components definition does not exclude intentional radiators.[74] By drawing primarily from a well-understood definition, we reduce the risks of industry confusion. We delegate to OET the authority to respond to questions as to what sort of components meet this definition and provide further clarifications.

47 CFR 15.3(k) Digital device. (Previously defined as a computing device)	**[NEW] 47 CFR 2.902 Logic-bearing hardware component.**
An unintentional radiator (device or system)	Any device, system, module, sub-assembly, integrated circuit, or other physical component
that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques;	that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques;
inclusive of telephone equipment that uses digital techniques	inclusive of telephone equipment that uses digital techniques
or any device or system	or any device, system, module, sub-assembly, integrated circuit, or other physical component
that generates and uses radio frequency energy for the purpose of performing data processing functions, such as electronic computations, operations, transformations, recording, filing, sorting, storage, retrieval, or transfer.	that generates and uses radio frequency energy for the purpose of performing data processing functions, such as electronic computations, operations, transformations, recording, filing, sorting, storage, retrieval, or transfer.

29. We reject several commenters' arguments that we adopt a broader prohibition on *all* components produced by entities identified on the Covered List, rather than just those that are logic-bearing hardware components.[75] For example, FDD urges the "Commission should prohibit the authorization of any equipment that contains *any* components produced by Covered entities "[76] While we agree, as we noted, with the spirit behind FDD's comments that we "should enact the broadest possible prohibitions to safeguard U.S. national security,"[77] we believe that our limit to logic-bearing hardware is more consistent with the Commission's underlying legal authority and national security goals. Logic-bearing hardware components pose a higher risk to national security because the computational logic they are capable of performing allows them to execute instructions and decisions that can enable surveillance, disruption and sabotage; the logic components can also accept firmware updates and respond to remote signals and activate dormant code in the future. We have also limited the prohibition to devices that operate above 9,000 pulses (cycles) per second, or 9kHz, which is the lowest frequency at which the Commission regulates spectrum for interference; this floor is consistent with our authority under Section

[74] *See* 47 CFR 15.3(k).

[75] See FDD Comments; Somos, Inc. Comments at 2-3; Telit Cinterion at 2.

[76] FDD Comment at 1 (emphasis added).

[77] FDD Comment at 2.

302 of the Communications Act to regulate the "interference potential of devices . . . capable of emitting [RF] energy . . . in sufficient degree to cause harmful interference."[78] By contrast, some components are "dumb," such as nails, paint, glue, or plastic structures, and pose no enhanced security concerns. This prohibition also does not apply to devices that operate above 9kHz but do not use digital techniques or generate and use RF for the purpose of performing data processing functions. Examples of devices not included in this prohibition would be fluorescent lights with electronic ballasts that run high-frequency oscillators above 9kHz to drive the lamp but do not have logic, or ultrasonic cleaners/ultrasonic transducers that oscillate above 9kHz but do not have logic.

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. For now, we limit our rule to hardware components, though we keep the record open on software and firmware components.

31. Many commenters opposed applying Covered List prohibitions to individual components other than modular transmitters, which necessarily includes opposing the rules we adopt today.[79] They opposed broad prohibitions because they could sweep in benign components, including those with no RF functionality, and argued that they would be technically impractical and administratively unmanageable.[80] We have addressed these concerns by including in our definition of logic-bearing hardware component only those components within our statutory authority to regulate under the Communications Act.[81] Our definition includes only devices that generate and use RF energy operate above 9 kHz, a threshold that marks the lower boundary of the regulated spectrum, and devices operating above 9kHz implicate the spectrum interference concerns .

32. Other comments opposed stating that some logic-bearing hardware components can perform various logical computing functions within a device, some of which may have nothing to do with the routing of user traffic.[82] We reject those arguments. Compromised logic-bearing hardware components may pose national security risks beyond the narrow situations envisioned by CTIA and other commenters. A compromised encryption logic chip, for example, may not route or redirect user data or directly permit visibility into user data; that compromised logic may lie dormant and undiscovered for years before hidden logic is triggered and pose a national security risk. Compromised logic can also cause a device to create power spikes or high-energy pulses that disrupt communications without routing data or eavesdropping user data; this can create national security risks beyond the narrow situations imagined by CTIA and other commenters. Compromised logic embedded in hardware, such as routers and modems, can enable threat actors to erase all data and disrupt communications, as happened in recent cyberattacks attributed to nation state actors.[83] These comments did not address the other statutory prongs, including posing unacceptable national security risk; any one of these prongs would be a reason for inclusion on the Covered List.[84] We also reject arguments that supply chain provenance tracking

[78] 47 USC § 302a(a).

[79] Garmin Comment at 4-8; ITI at 4; Sony at 2; USTelecom at 7; CTIA at 8-9.

[80] Incompas Comment at 2; ITI Comment at 3; Hikvision Reply at 21.

[81] 47 USC 302a(a) (granting the Commission authority to regulate the "interference potential of devices which in their operation are capable of emitting radio frequency energy . . . in sufficient degree to cause harmful interference").

[82] CTIA Comments at 13-14.

[83] Juan Andres Guerrero-Saade and Max van Amerongen, *Sentinel Labs*, AcidRain: A Modern Wiper Rains Down on Europe, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (Mar. 31, 2022).

[84] *Id.* at § 1601(b)(2)(A)-(C) ("[§ 1601(b)(2)(A)] . . . permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; *or* [§ 1601(b)(2)(B)] causing the network of a provider of advanced communications service to be disrupted remotely; *or* [§ 1601(b)(2)(C)] otherwise posing an unacceptable (continued….)

would be unworkable.[85] Our prohibition here applies only to those logic-bearing hardware components produced by Covered List entities. The compliance burden here would be consistent with the practices recommended by NIST in the Cybersecurity Supply Chain Risk Management Practices for Systems, which includes the use of bills of materials that identify logic-bearing hardware components. The use of hardware bills of materials (HBOM) is common in modern supply-chain risk management practices.[86]

33. We also reject certain commenters arguments that the Commission should adopt a more limited list of components or not adopt any further component restrictions at all.[87] We disagree with CTIA's contention that we should limit ourselves to only those components that can "route or redirect user data traffic or permit visibility into any user data or packets," as consistent with Section 8 of the National Defense Authorization Act of 2019 and the Secure Networks Act.[88] For one thing, the Secure Networks Act does not limit additions to the Covered List to devices that pose specific national security risks concerning user data or packets, but also includes devices that "otherwise pos[e] an unacceptable risk to the national security of the United States or the safety and security of United States persons."[89] For another thing, the Commission only applies the restrictions we adopt today to logic bearing hardware incorporated into communications equipment requiring FCC authorization. This targeted addition responds to record suggestions to focus on components with direct impact on communications functions, which we find includes disruption and interference of communications as well as traditional espionage, surveillance, and interception concerns, while avoiding prohibitions on components further removed from Covered List determinations.[90] As we explain above, logic-bearing hardware components are not "components with no RF functionality" divorced from the national security determinations;[91] a Covered List entity can compromise logic-bearing hardware inside communications equipment just as it can compromise a whole device. including those with no RF functionality.

34. Furthermore, we recognize that, as some commenters note, these prohibitions may impose compliance costs on device makers. However, we believe these costs are outweighed by the national security benefits of protecting the nation against devices that might pose "unacceptable risks to the national security of the United States or the safety and security of United States persons."[92] Device

---

risk to the national security of the United States or the security and safety of United States persons.") (emphasis added).

[85] *See, e.g.,* Hikvision Reply Comments at 15 (citing ITI, US Telecom, Garmin, CTIA comments).

[86] Somos, Inc at 6*; see also* Lucas Tate, et al., *Comparing Bills of Material,* Pacific Northwest National Laboratory (2024), https://arxiv.org/pdf/2411.10384 ("Recently, BOMs have been gaining traction as a tool to increase our supply chain understanding and help respond to this threat."); Seth Carmody, et al., *Building resilient medical technology supply chains with a software bill of materials,* npj Digit. Med. 4, 34 (2021), https://doi.org/10.1038/s41746-021-00403-w ("An example of effective application of the SBOM concept comes from the financial services industry. By 2015, a series of software supply-chain vulnerabilities had forced the industry to re-evaluate the third-party software in its infrastructure. This sector quickly adopted SBOM concepts into their internal development and procurement processes. Now, if a vendor can provide an SBOM, it serves as a litmus test for the maturity of the vendor's organization. If vendors lack an SBOM, many financial services organizations anticipate that their products will likely cost more to evaluate, operate, and own over their lifecycles. As a result, the financial organizations might negotiate discounts to account for these increased costs.").

[87] Commercial Drone Alliance Comments at 2-3, CTIA Comments at 8-12, NCTA Comments at 4-5, Garmin Comments at 4-8.

[88] CTIA comment at 11-14.

[89] 47 USC 1601(b)(2)(C).

[90] CTIA Comment at 10; Motorola Comment at 5; Garmin Comment at 4.

[91] See ITI Comment at 3 (warning the Commission against this overbreadth); *see also* Sony Comment at 1.

[92] 47 USC § 1601(b), (c); *EA Security 2d R&O* at 45 ("[I]t is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (quoting *Haig v. Agee*, 433 U.S. 280, 307 (1981)).

makers that incorporate untrusted logic-bearing hardware components because they fail to maintain a supply chain risk management program with visibility into such components, including by using bills of materials, simply pass those costs onto the end users of the devices. Those costs are not merely financial. End users ultimately absorb the costs and risks created by device makers seeking to cut compliance costs. End users must bear the risks of surveillance, data exfiltration, and disruption that can be created by compromised logic-bearing hardware components that end users have no ability to inspect or audit. An end user purchasing a connected device has no visibility into whether its logic bearing components originate from untrusted entities named on the Covered List. We believe the device maker that bears a one-time compliance cost to vet its supply chain is the more appropriate party to bear these costs, rather than placing the costs the downstream end user.

35. We also believe that many of the commenters' expressed legal and practical concerns with the breadth of the component part proposals in the FNPRM is alleviated by the fact that we decline at this time to take action on devices containing certain components produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.[93] There is minimal record evidence in support of such action, and the commenters made clear the enormous practical challenges with this proposal[94]. But we keep the record open on these points.

36. One commenter urges the Commission to add to the Covered List all entities Congress identified in section 5949 of the FY2023 National Defense Authorization Act (NDAA) (all semiconductor producers subject to government procurement restrictions) just as the Covered List currently contain communications equipment and services contained in Section 889 of the FY 2019 NDAA.[95] The Commission lacks the authority to add to the Covered List on its own initiative.[96] However, we note that, pursuant to the rules we adopt today, if an enumerated source for making specific determinations for the Covered List[97] makes a determination about communications equipment produced by entities identified in section 5949, the Commission would "prohibit authorization of any device containing their chips."[98]

B. Components Prohibitions Limited to Producer/Provider-Based Determinations

37. We emphasize that the prohibitions recognized and adopted today apply only for logic-bearing hardware components produced by an entity identified on the Covered List. They do not apply to components produced by entities that produce equipment subject to recent production location-based additions to the Covered List – such as components produced by entities that also produce UAS, UAS critical components, or routers in a foreign country – unless that entity is otherwise identified on the Covered List (for example, because they are identified in Section 1709 of the FY25 NDAA).[99]

38. We further determine that this prohibition is effective as of adoption of this Order, with no transition period as the change only impacts new equipment authorizations. We direct OET to advise Telecommunication Certification Bodies (TCBs) of this change. This prohibition applies immediately for applications in process; pending applications may be amended applications to substitute components. This change is prospective, and does not affect previously authorized equipment, which may continue to be marketed, imported, and used pursuant to its existing authorization. We find good cause to make this

[93] David Feith and Michael Sobolik Comments at 2.

[94] Commercial Drone Alliance Comments at 2-3, CTIA Comments at 8-12, NCTA Comments at 4-5, Garmin Comments at 4-8.

[95] Chris McGuire Comment at 2, 6-9.

[96] 47 USC § 1601.

[97] 47 USC § 1601(c).

[98] Chris McGuire Comment at 2.

[99] *See* List of Equipment and Services Covered by Section 2 of the Secure Networks Act, FCC.gov, https://www.fcc.gov/supplychain/coveredlist (last visited May 20, 2026); FY25 NDAA § 1709, Pub. L. No. 118-159, 138 Stat. 1773, 2209–11 (to be codified as Note to 47 U.S.C. § 1601).

restriction effective immediately,[100] because devices containing these components may pose similar "unacceptable risks to the national security of the United States or the safety and security of United States persons"[101] that covered equipment does, which outweighs any temporary disruption. This is similar to the approach we took in the *First EA Security R&O*, which adopted an immediate freeze on all authorizations for any device produced by Covered List entities, effective upon release of the Report & Order.[102] Furthermore, these entities have long been flagged as national security risks; responsible supply chain risk assessments should have identified and mitigated risks from these entities. Finally, allowing for a lengthy transition period would allow device makers to flood the market with potentially compromised devices.

C. Marketing

39. The *Second Further Notice* sought comment on how the Commission could strengthen its efforts to prevent unauthorized marketing of equipment.[103]

1. Clarifying "distribution for the purpose of selling" as part of marketing

40. In the *Second Further Notice,* the Commission sought comment on clarifying the term "distribution for the purpose of selling" as used in the definition of "marketing" under our rules.[104] We sought comment on whether activities typically engaged in by online marketplaces, such as consignment, warehousing, inventory management, order processing, labeling, packaging, billing, and other fulfillment services, individually or collectively, would constitute marketing activities under our rules.[105] We specifically sought comment on how a definition of "distribution" might affect various entities that are not themselves engaged in directly selling RF equipment but participate in the distribution of RF equipment.[106]

41. Commenter Sirius XM supported clarifying that activities typically engaged in by online marketplaces (e.g., consignment, warehousing, inventory management, order processing, labeling, packaging, billing, and other fulfillment services) are performed in connection with selling devices and constitute "distribution for the purpose of selling."[107] Sirius XM supports clarifying that the definition of marketing is met when products are shown on online marketplaces, sold through platforms, or delivered to customers with the involvement of these platforms, and such online marketplaces should be held liable.[108] Sirius XM further notes that the definition of marketing is met by online marketplaces that display devices, allow them to be purchased by clicking on the platform, or play a role in transferring possession of the device to customers, and supported holding those platforms liable for marketing. In other words, these commenters propose that marketing occurs regardless of whether the online marketplace in question is marketing its own products or a third-party's products.

42. Hikvision USA opposes interpreting the scope of distribution in a way that includes intermediary transporters and warehouses, stating that section 302 of the Communications Act expressly exempts "carriers transporting such devices or home electronic equipment and systems without trading in

[100] *See* 5 U.S.C. § 553(d)(3).

[101] 47 U.S.C. § 1601(b)(1).

[102] *EA Security First R&O* at paras. 264-66.

[103] *Second Further Notice,* paras. 84-89.

[104] *Second Further Notice,* para. 89 (quoting 47 CFR § 2.803(a)).

[105] *Id.*

[106] *Id.*

[107] Sirius XM Comment at 2.

[108] *Id.*

them."[109] CTIA likewise cautions that "it is not clear that an entity that does not take title to a device could reasonably be held to be distributing a device for the purpose of selling that device as section 2.803 of the Commission's rules requires, since an entity that does not have title to the device cannot itself sell the device. Moreover, "a broad interpretation runs the risk of ensnaring logistics companies and shippers like FedEx or UPS, who are clearly not 'marketing' devices."[110] Other commenters generally cautioned against an expansive interpretation of the definition of marketing, noting that such interpretations "could work a sea change in the way in which products are sold in the United States, and thus deserves careful consideration."[111] These comments did not specifically address the indicia of distribution raised in the *Second Further Notice* (e.g., consignment, warehousing, inventory management, order processing, labeling, packaging, billing, and other fulfillment services); rather, they raised policy arguments against holding online marketplaces liable for marketing. These comments are discussed in more detail in the section below (Section III.B.3) but are not relevant here as to the threshold definition of distribution under our rules.

43. *Discussion.* We have considered comments cautioning against an expansive interpretation of our marketing rules. We agree with Hikvision USA and CTIA that a carrier transporting unauthorized devices without trading in them is outside the scope of section 302 of the Communications Act. Section 302(c) of the Act provides, in relevant part, that the Commission's equipment marketing rules "shall not be applicable to carriers transporting such devices or home electronic equipment and systems without trading in them…."[112] We find that our marketing rules do not cover a carrier's transport of unauthorized devices in isolation. This conclusion does not, however, preclude enforcement against an online marketplace whose role in a transaction extends beyond mere carriage—including by listing on a website, warehousing, advertising, or processing payment.

44. We further find that the term "distribution for the purpose of selling" should encompass the listing of regulated equipment on an online marketplaces, in combination with any of the following activities: consignment, warehousing, inventory management, order processing, labelling, packaging, billing, or fulfilment services – even if that equipment is sold or offered for sale by a third-party seller. An analogous statute, the Consumer Product Safety Act, has long provided that, "[t]he terms 'to distribute in commerce' and 'distribution in commerce' mean to sell in commerce, to introduce or deliver for introduction into commerce, or to hold for sale or distribution after introduction into commerce."[113] The Consumer Product Safety Commission (CPSC) unanimously interpreted the plain meaning of "distribution in commerce" to cover many of the same activities on which we sought comment on in the *Second Further Notice* when performed by online marketplaces.[114] For example, the CPSC found that activities such as consignment,[115] warehousing,[116] inventory management, order processing, labelling,

[109] Hikvision Comments at 40 (quoting 47 U.S.C. § 302a(c)).

[110] CTIA Comments at 24, n. 63.

[111] CTIA Comments 24; NTCA Comments at 6-7.

[112] 47 USC § 302a(c).

[113] 15 U.S.C § 2052(a)(7).

[114] *Amazon.com, Inc.*, CPSC Docket No. 21-2, Decision and Order (July 29, 2024), *available at* https://www.cpsc.gov/s3fs-public/pdfs/recall/lawsuits/abc/142%20-%20In%20the%20Matter%20of%20Amazon.com%20Inc.%20Decision%20and%20Order.pdf (finding Amazon's online marketplace activities qualified as "distribution in commerce") [https://perma.cc/U3QQ-4QAS]. Amazon has challenged the CPSC interpretation. *Amazon.com, Inc. v. CPSC,* No. 25-cv-853 (D. Md. filed Mar. 14, 2025).

[115] CPSC Order at 28 ("Fulfilled by Amazon participants send their products to Amazon, not directly to customers who order through Amazon.com, with the intention and expectation that they will be sold to end customers.")

[116] *Id.* ("Amazon stores the Fulfilled by Amazon products in its fulfillment centers until a customer purchases the product on Amazon.com, at which point Amazon fulfills the order and ships the product to the customer . . .

(continued….)

packaging, billing, and other fulfilment services[117] constituted "distribution in commerce" when performed by an online marketplaces in connection with sales of defective products on its website. Like section 302(c) of the Communications Act, the Consumer Product Safety Act exempts carriers who act "*solely* by reason of receiving or transporting a consumer product in the ordinary course of business as such a [common] carrier or [freight] forwarder."[118] Therefore, we find that the plain meaning of the term "distribution for the purpose of selling" includes the listing of regulated equipment on an online marketplace, in combination with consignment, warehousing, inventory management, order processing, labelling, packaging, billing, or fulfilment services. We further find that the carveout in Section 302(c) for carriers transporting devices does not exempt online marketplaces involved in the ultimate sale of such devices. While we find the CPSC's construction of the analogous term "distribution in commerce" instructive, our holding does not depend on it. We conclude that the best reading of "distribution for the purpose of selling" in our rules, and of the underlying statutory authority in Section 302(b), independently reaches the fulfillment activities described above.[119]

45. The Commission also clarifies that, online marketplaces that list third-party products on their platforms are engaged in marketing because they are engaged in "offering for sale" under our marketing rules.[120] An ordinary person understands an online marketplace to be "offering for sale" the goods available for purchase on its platform, even if third-party sellers ultimately hold title to the products.[121] Of course, online marketplaces also frequently engage in "advertising for sale" of third-party products, and sell keyword search terms funneling customers toward these products, which also expressly brings them within our existing marketing rules.[122] We conclude that the ordinary meaning of "offering for sale" reaches a party that presents a product to prospective buyers and enables its purchase, irrespective of which party holds title to the goods.

46. We therefore amend section 2.803(a) of our rules to clarify that entities are engaged in "marketing" when they list equipment on an online marketplace, in combination with any of the following activities: consignment, warehousing, inventory management, order processing, labelling, packaging, billing, or fulfilment services – even if that equipment is sold or offered for sale by a third-party seller.

2. Online marketplaces that "market" unauthorized devices are subject to enforcement

47. The *Second Further Notice* sought comment on steps to strengthen the Commission's ability to enforce its marketing rules, and ensure more accountability among resellers or drop shippers of

Fulfilled by Amazon participants pay Amazon monthly and long-term storage fees for Amazon to store their products in its fulfillment centers.").

[117] *Id.* ("If Amazon does not hold the product (e.g., it is out of stock), customers cannot complete the transaction, indicating that Amazon must have the product in its warehouse—to hold for sale—before the sales transaction can occur.").

[118] 15 U.S.C. § 2052(b) (emphasis added).

[119] 47 CFR § 2.803(a); 47 USC § 302a(b).

[120] 47 CFR § 2.803(a).

[121] *Cf. Lacks Indus., Inc. v. McKechie Vehicle Components USA, Inc.*, 322 F.3d 1335, 1347 (Fed. Cir. 2003) (interpreting "offer for sale" in the context of the patent law test for the on-sale bar to mean "an offer which rises to the level of a commercial offer for sale, one which the other party could make into a binding contract by simple acceptance (assuming consideration)" (quoting *Grp. One, Ltd. v. Hallmark Cards*, 254 F.3d 1041, 1048 (Fed. Cir. 2001); *Powers v. Coffeyville Livestock Sales Co., Inc*., 665 F.2d 311, 312 (10th Cir. 1981) (finding an auctioneer to be a seller of goods under the Uniform Commercial Code and that "[c]ertainly an auctioneer sells goods, although generally as an agent for someone else")

[122] *See* 47 CFR § 2.803(a).

covered equipment for compliance with the marketing rules.[123] We also sought comment on additional obligations that should be imposed on retailers, sellers, and re-sellers, e-commerce websites, distributors, or advertisers to ensure that the public is aware of the authorization status of RF equipment.[124] We noted that while we have not previously focused past enforcement efforts on commercial consignees, the Commission tentatively concluded that "retailers and commercial consignees are typically better equipped to verify equipment compliance than consumers who might mistakenly assume that a marketed product is compliant."[125]

48. Sirius XM strongly supports clarifying that e-commerce platforms are subject to the marketing rules, and bear responsibility for:

> ensuring that all products shown on their platforms, sold through their platforms, or delivered to consumers with the involvement of their platforms . . . are in fact FCC certified. . . If a device subject to FCC requirements is displayed on an e-commerce platform, purchased by clicking on the platform, or if the platform plays a role in transferring possession of the device to customers, then the platform must bear responsibility for verifying the FCC certification and labeling of that device." [126]

49. CTA notes that retailers, platforms, and other service providers generally do not have access to regulatory authorization or compliance records held by manufacturers.[127] NTCA noted similar concerns about the burdens on retailers.[128] The Center for Regulatory Freedom (CRF) likewise opposed holding liable resellers and distributors, who may lack technical awareness or practical control over equipment design or sourcing, and proposed that marketing or distribution liability definitions be tethered to actual knowledge, intent, knowledge and control.[129]

50. *Discussion:* We find that online marketplaces, to the extent they market unauthorized devices, are subject to enforcement of our marketing rules. Section 302 of the Communications Act unambiguously prohibits a "person" from selling, offering for sale, or shipping devices that do not comply with our rules governing equipment, without regard to whether the person is a manufacturer of such equipment, an online marketplace, or other such person.[130]

51. We have considered and decline to adopt proposals to limit marketing liability to those bad actors who willfully or intentionally violate the marketing rules. We note that there is no willfulness or intent element of the prohibited activities in our marketing rules or in Section 302a(b) of the Communications Act. [131]

---

[123] *Second Further Notice* at para. 85.

[124] *Id.* at para. 91.

[125] *Id.* at para. 88.

[126] Sirius XM Comment at 2.

[127] CTA Comment at 11

[128] NTCA Comment at 7 (similar concerns);

[129] Center for Regulatory Freedom (CRF) Comments at 9.

[130] 47 U.S.C. § 302a(b).

[131] *See* 47 USC § 302a(b). Though even an incidental infraction of the equipment marketing rules may create liability, the Commission will fully consider in determining any forfeiture liability the circumstances attendant to a particular violation, including the extent to which an entity intentionally violates the rules, pleads willful ignorance, or implements robust best practices to strengthen its compliance regime. *See* 47 CFR § 1.80(b)(11) (citing degree of culpability and other factors considered when determining the amount of a forfeiture liability). . Moreover, the Act's enforcement provisions provide for enforcement of the Commission's rules against entities that hold no FCC authorizations so long as the Commission sends a citation of the violation and an opportunity to cease the activity

(continued….)

52. We have also considered downstream supply chain participants (retailers, resellers, distributors, e-commerce platforms), which might not have the same level of access to technical compliance information that a manufacturer or designer may have, and decline to exempt these entities from enforcement. While commenters noted that online marketplaces might struggle to verify equipment compliance,[132] no commenter disputed the tentative conclusion in the *Second Further Notice* that online marketplaces are typically better able to verify equipment compliance than *consumers*. Online marketplaces have greater resources than consumers do to access compliance resources such as the Commission's equipment authorization websites, as well as commercially available supply chain databases. Online marketers have front-end access to search the Commission's public available Equipment Authorization System database; they also have back-end access to Application Programming Interfaces (APIs) to verify FCC IDs.[133] They can confirm which devices have valid authorizations or FCC IDs because of the Commission's rules require FCC IDs to be displayable via a physical label, e-label, or on the packaging/manual. They can also require proof of regulatory compliance (including SDoC authorizations) in their commercial agreements with suppliers and otherwise have a greater ability to negotiate with upstream suppliers than consumers. Expressly exempting online marketplaces from any marketing liability would allow them to receive the benefits, and profits, of marketing unauthorized equipment while passing all the costs on to consumers. Those costs to consumers are real; consumers must bear the risk of unknowingly purchasing unauthorized equipment that may not be legally used in the U.S., emits harmful or disruptive interference or, by virtue of being on the Covered List, poses "unacceptable risk to the safety and security of United States persons."[134] Placing liability on online marketplaces that market unauthorized equipment ensures that these participants in the supply chain are incentivized to safeguard consumers.

3. Requiring online marketplaces to display FCC IDs

53. In the *Second Further Notice*, we sought comment on explicitly requiring online marketplaces to display the FCC ID at the online point of sale.[135] The Commission currently requires that each certified device display its FCC ID on the device or within an integrated display.[136] An FCC ID uniquely identifies the device and is registered to the party responsible for ensuring that each unit marketed continues to comply with the Commission's rules. A valid FCC ID is recorded in the Commission's publicly-accessible Equipment Authorization System (EAS) database.

54. Feith and Sobolik are supportive of this requirement, noting that requiring the FCC ID would be broadly beneficial with minimal burdens.[137] By contrast, CTA opposes new marketing requirements such as mandatory FCC ID display at online points of sale, arguing the measures would impose heavy burdens without meaningful security benefits and could confuse consumers.[138] Other commenters opposed requiring FCC IDs to be included on printed packaging, citing the burden and cost of doing so.[139]

---

before serving a Notice of Apparent Liability. *See* 47 U.S.C. § 503(b)(5).

[132] Consumer Technology Association Comments at 8-9; CTIA Comments at 18.

[133] Office of Engineering and Technology, Federal Communications Commission, EAS Web API Services (describing the GetFCCIDList API), 2026, https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=50070&switch=P.

[134] 47 U.S.C. § 1601(b)(2)(C); 47 CFR § 1.50002(b)(2)(iii).

[135] *Second Further Notice* at paras. 91, 93 (referring to e-commerce sites and online retailers).

[136] 47 CFR §§ 2.925, 2.926, 2.935.

[137] David Feith and Michael Sobolik Comments at 2.

[138] CTA Comments at 10-12.

[139] Sony Comments at 2-3; ITI at 6.

55. *Discussion*: We find that requiring the display of FCC IDs at the online point of sale will not only strengthen FCC enforcement of marketing prohibitions which is needed to counterbalance the national security risks associated with covered equipment, but also allows consumers to make informed purchasing decisions. The FCC ID exists to promote transparency, reduce confusion regarding the authorization status of devices, and aid the Commission's duty to ensure safe communications networks.[140] The presence of the FCC ID signals that a device has been authorized; i.e., it has been properly tested, demonstrated its compliance with the Commission's technical standards, and satisfied all other requirements for certification.[141] Through the EAS database, the public may verify whether a particular device is certified by searching the EAS database for the FCC ID. Consumers, retailers, distributors, and other supply chain entities can verify that that they are purchasing and marketing devices that are authorized for sale within the United States and are safe products.

56. Although equipment authorized pursuant to SDoC currently does not have an FCC ID, and so cannot be verified within any public database, our rules do currently require that the device include a compliance information statement at the time or marketing or importation.[142] The compliance information statement identifies both the device model and the party within the United States that is responsible for its compliance.[143] However, in the past, checking the FCC ID or compliance information statement typically required that a device be physically inspected, which meant that consumers often could not determine whether a device is authorized until *after* an online sale has been consummated.

57. We find that it is crucial that the FCC ID and compliance information statement be displayed at the online point of sale, including in any online advertisement, to advise the public whether RF products are in fact authorized. We agree with Feith & Sobolik that "[r]equiring FCC ID disclosure in product listings would clarify equipment authorization before a transaction occurs."[144] We further find that marketing entities must verify the FCC ID before displaying it. Online marketplaces must obtain and prominently display the correct FCC ID of a certified device at the online point of sale. Online point of sale marketing for equipment that is authorized by certification must include the FCC ID. Moreover, online marketplaces may be held liable for the failure to properly display the correct FCC ID.[145]

58. Since its adoption in 1979, section 2.925(d) of the Commission's rules has required that the FCC ID be permanently affixed to the device and be "readily visible to the purchaser at the time of purchase."[146] Because online purchases now account for over 70 percent[147] of consumer electronics sales today, the amendment we adopt here refreshes the scope of the rule and restores its original intent. The amended rule also aligns now with similar requirements under our rules that require the provision of

[140] 47 C.F.R. § 2.925(a)(1); 47 C.F.R. § 2.926(e).

[141] 47 CFR § 2.926(e) ("No FCC Identifier may be used on equipment to be marketed unless that specific identifier has been validated by a grant of equipment certification.").

[142] 47 CFR § 2.1077(a). We also seek comment in the *Further Notice* on requiring registration and display of FCC IDs for SDoC-authorized products. *See, supra*, at para. 115.

[143] 47 CFR § 2.1077(a).

[144] David Feith and Michael Sobolik Comments at 2.

[145] We acknowledge that any website can temporarily experience downtime but decline, at this time, to establish rigid criteria to define the term "readily accessible."

[146] 47 CFR § 2.925(d); *see also* 47 U.S.C. 302a, 303(r).

[147] Digital Commerce 360, Consumer Electronics Ecommerce Statistics, ("Revenue in consumer electronics . . . Online penetration was very high, at 72.9% in 2023. That's an increase of about 7% from 2022, when penetration was 68.2%."). https://www.digitalcommerce360.com/consumer-electronics-ecommerce-statistics/, last visited June 26, 2026.

certain information at the time of marketing.[148]

59. We agree with Feith & Sobolik that requiring FCC ID at point of sale is "a minimally invasive standard of compliance that would increase transparency, enforcement, and security."[149] We have considered and rejected CTA's comments opposing this requirement. CTA contends that requiring the FCC ID in an online product listing could be burdensome; however, it has provided no facts in the record upon which we could begin to assess this claim, and no other entity has supported this claim. We do not find that requiring compliance information within a product listing would present a burden. Online marketplaces almost uniformly display product specifications, descriptions, consumer reviews, and hyperlinks within a product listing webpage and generally already display production information of comparable complexity, such as model numbers, UPC codes, and regulatory marks for other agencies. Online marketplaces also tend to require that third-party sellers provide certain minimal information within a listing regarding the product marketed. Online marketplaces already display product specification information. We believe that implementing this requirement should be straightforward and would likely include updating the HTML code of any product page, revising any terms of service agreements, and modifying a platform's back-end infrastructure to accommodate the new requirement, all of which are routinely performed in the normal course of business. Moreover, to the extent that online marketplaces have not previously taken steps to ensure that products they market to U.S. consumers are lawful, these measures are both necessary and long overdue. In our experience, we have found that requiring FCC IDs at the online point of sale for online marketplaces would support compliance efforts by enabling platforms to leverage automated controls to screen for unauthorized equipment.[150] We therefore revise our rules to expressly require that online marketplaces display the correct FCC ID of all certified devices at the online point of sale.

60. In the *Second Further Notice*, we also sought comment on whether certain entities should be required to display a certified device's FCC ID number so that it is visible on the outside of the device's packaging.[151] We posited that such a requirement could make it easier for consumers to verify a device's authorization status.[152] Similarly, the lack of a valid FCC ID on consumer packaging or bulk shipments, for devices that must be authorized by certification, can act as a litmus test that enables swift enforcement. For instance, U.S. Customs and Border Protection (CBP) could easily identify and seize equipment that lacks a valid, required FCC ID at the border, before it reaches online marketplaces and consumers. We have also considered comments opposing including FCC IDs on the external product packaging[153] but based on the record we do not adopt such proposals at this time, though we keep the record open on this point should members of the public or industry wish to comment.

D. Clarifications regarding Modifications Such that Previously-Authorized Equipment Would Become Covered

61. In the *First Report and Order*, the Commission revised its rules to require that all applicants that request a modification to any previously certified equipment authorizations must include

[148] Devices that display their FCC ID electronically must also display it on the device or its packaging or display other information (such as a model number and identification of a Web page that hosts the relevant regulatory information) that permits the devices to be identified "at the time of importation, marketing, and sales." 47 CFR § 2.935(f). Similarly, SDoC compliance information must be provided "at the time of marketing or importation." *Id.* at 2.1077(a). We acknowledge that marketing is already defined in section 2.803(a) to include the elements of sale and importation.

[149] David Feith and Michael Sobolik Comments at 2.

[150] *See, e.g.,* Chairman Carr Announces Initial Success of "Operation Clean Carts," News Release, FCC.gov (Oct. 10, 2025), https://www.fcc.gov/document/chairman-carr-announces-initial-success-operation-clean-carts.

[151] *Second Further Notice* at para. 91.

[152] *Second Further Notice* at para. 91.

[153] Sony Comment at 2-3; Sony Comment as 13; ITI Comment at 6.

written certifications that authorization of the equipment is not prohibited under section 2.903 and regarding whether or not the applicant is identified on the Covered List.[154] The Commission further modified its rules to reinforce this prohibition and prevent companies on the Covered List from using the SDoC process to authorize any of their equipment. Instead, Covered List entities must use the more rigorous certification process, which gives the Commission greater oversight and helps prevent authorization of equipment that could pose national security risks.[155] In the *Second Report and Order*, the Commission clarified that the intent of these rule changes was to prohibit any modification to equipment that is already covered or would become covered as a result of a modification, consistent with the Secure Equipment Act's ban on reviewing or approving applications for covered equipment. This prohibition also applies to permissive changes that do not require a formal application, such as class I permissive changes that are "approved by rule."[156] The Commission therefore amended its rules in sections 2.932(b) and (c) and 2.1043(b) to state that permissive changes may be made "[e]xcept for equipment prohibited from authorization pursuant to § 2.903,"[157] the rules section prohibiting the authorization of covered equipment.

62. SZ DJI Technology Co. Ltd. (DJI) opposes any blanket prohibition of permissive changes or modifications to authorized DJI products already in the U.S. market.[158] DJI cited the need for "firmware updates . . . to strengthen data security and for important safety updates that ensure products can continue to be operated safely and that a blanket prohibition could prevent end users from making the necessary updates, making the equipment and U.S. airspace less safe."[159] MEMA, the Vehicle Suppliers Association, similarly recommended that the Commission expressly exclude routine over-the-air (OTA) firmware and software updates used by vehicle suppliers to remediate cybersecurity vulnerabilities, address safety defects, and maintain regulatory compliance, such as in recall scenarios.[160] We have considered these comments, and find such concerns can be addressed through limited waivers, as we have already done to allow previously-authorized UAS and routers to receive such updates.

63. The Commission clarifies its rules regarding permissive change modifications. As we stated in the *Second Report and Order*, "the intent of the Commission in adopting these provisions was to prohibit modification, including permissive changes, to previously authorized covered equipment *or equipment that would become covered as a result of such modification or permissive change*."[161] We amended our rules to expressly prohibit modifications to equipment that is prohibited from receiving authorization as covered equipment.[162] In the *Second Further Notice*, we sought comment on "additional action we might take to further strengthen and streamline our efforts to identify covered equipment and ensure it is not authorized."[163] We now revise section 2.932 and 2.1043(b) to make clear the Commission's intent in its *First* and *Second Report and Order* that prohibition applies to both equipment that is already prohibited from receiving equipment authorization pursuant to section 2.903, as well as equipment that would become prohibited pursuant to 2.903 as a result of the change.

---

[154] 47 CFR §§ 2.932(b), 2.1043(b)(2)(i)(B), (C).

[155] 47 CFR § 2.906(d).

[156] *See* 47 CFR § 2.1043(b)(1) ("A Class I permissive change includes those modifications in the equipment which do not degrade the characteristics reported by the manufacturer and accepted by the Commission when certification is granted.").

[157] 47 CFR § 2.932(b); *id*. § 2.1043(b) (using identical language); *see also* § 2.939(c)(2).

[158] SZ DJI Technology Co. Ltd. Comment at 1 (Jan. 5, 2026)

[159] *Id.*

[160] MEMA Comments at 6-7.

[161] *Second Report and Order* at para. 55 (emphasis added).

[162] 47 CFR §§ 2.932, 2.1043(b)

[163] Second Further Notice at para. 82.

64. This prohibition applies to any "change in the design, circuitry or construction of any equipment or device for which an equipment authorization has been issued."[164] A few examples are illustrative. If a device was originally produced by Entity A, that device may not be subsequently redesigned and produced by Entity B if Entity B is a Covered List entity. If a UAS was certified at a time at which the UAS was produced in the United States, the device cannot later be modified by transferring production of the device to a foreign country, which would render the UAS "covered."[165] If a UAS device is certified because it meets the "domestic end product" definition,[166] the UAS may not subsequently be modified by altering the componentry in such fashion that the modified device would not meet the "domestic end product" definition. For the avoidance of doubt, routine software and firmware security authorized until January 1, 2029, by the OET waivers referenced in Section II.C above,[167] do not constitute prohibited modifications under this paragraph.

65. Several commenters caution that determining whether a modification changes the "production" source or component composition of a device may be technically complex or burdensome, particularly given global supply chains and the evolving meaning of "produced by."[168] We emphasize that modification prohibitions apply only when an applicant makes a change that means that the equipment, as modified, meets the criteria of becoming "covered" equipment. We are not, at this time, imposing additional obligations on applicants to investigate component lineage beyond what is ordinarily required for compliance with the equipment authorization rules. The Commission will not deem a device prohibited unless the modification itself renders equipment "covered" equipment.

66. For purposes of Covered List implementation in the equipment authorization program, the Commission clarifies that, for all modifications, the term "produced by" for the purpose of producer/provider-based Covered List additions shall continue to be evaluated under the totality of circumstances, including substantial responsibility or control over design, development, manufacture, or assembly. For example, a device assembled by a Covered List entity is "produced by" that entity; the presence of otherwise authorized components does not alter covered status. Similarly, a device that is covered remains covered regardless of whether it uses components that individually hold valid equipment authorizations. Permitting a Covered List entity to assemble a device using authorized components would enable circumvention of our rules and is incompatible with the "produced by" standard, which looks to substantive involvement in production rather than the authorization status of sub-components.[169]

E. Re-Certifications Required of Covered List Entities for Any Change to Equipment

67. In the EA Security Second Further Notice, the Commission proposed the submission of recertification for any equipment for which an entity identified on the Covered List seeks modification for a permissive change. The Commission explained that this proposal was consistent with the Commission's longstanding "intent to require one procedure for all equipment authorization applications made by" Covered List entities. The Commission asked for input on how these requirements might enhance supply chain security, whether a streamlined process should be created, and what impacts or burdens this might place on the supply chain and how those could be reduced.

---

[164] 47 CFR § 2.932(a).

[165] *See* Federal Communications Commission, List of Equipment and Services Covered by Section 2 of the Secure Networks Act ("Covered List"), https://www.fcc.gov/supplychain/coveredlist, last visited June 26, 2026.

[166] *See* Federal Communications Commission, List of Equipment and Services Covered by Section 2 of the Secure Networks Act ("Covered List") ("UAS … produced in a foreign country—except… UAS that qualify as 'domestic end products' under the Buy American Standard, 48 CFR 25.101(a), until January 1, 2027")., https://www.fcc.gov/supplychain/coveredlist, last visited June 26, 2026.

[167] *See supra, at para. 12.*

[168] CTA Comment at 4; USTelecom Comments at 4-5.

[169] David Feith and Michael Sobolik Comments at 1-2.

68. The record in this proceeding reflects broad agreement that modifications to firmware, software, or other functional elements of Covered List equipment can materially alter the device's security posture. FDD strongly supports requiring full recertification for any modification made by a Covered List entity, arguing that this is necessary to prevent post-authorization tampering and maintains that such a requirement directly enhances supply-chain security by pushing U.S. companies toward more trustworthy suppliers. Other commenters stress that any requirement for recertification must be strictly tethered to a "specific determination" by one of the Enumerated Sources identified in the Secure Networks Act.

69. To ensure the continued protection of U.S. networks and infrastructure and ensure that there is one procedure for all equipment authorization applications made by Covered List entities, the Commission determines that all Covered List entities that seek permissive change modifications to covered or non-covered equipment must submit applications for recertification. For the avoidance of doubt, this requirement applies only when the applicant for the permissive change is itself an entity identified on the Covered List. A non-Covered List manufacturer that modifies equipment originally produced by a Covered List entity, where the modification does not result in the modified device being 'produced by' the Covered List entity under the totality-of-the-circumstances framework, is not subject to this recertification requirement. Under this approach, we affirm that no Covered List entity is permitted to rely on the SDoC process for modifications, even for non-covered equipment regardless of the nature or scope of the change. This is analogous to the certification requirement adopted in the First Report and Order, prohibiting Covered List entities from using the SDoC process in order to ensure a single equipment authorization procedure for such entities.

70. We note that this requirement only applies to Covered List entities and therefore does not apply to the production location-based entries on the Covered List, including foreign-produced UAS, UAS critical components, and routers, because this requirement is designed to give the Commission oversight over modifications made by specific entities that pose national security risks.

71. We also note that OET previously granted limited waivers permitting Class I and Class II permissive changes for Covered List UAS equipment and Covered Routers through January 1, 2029 in order to allow continued delivery of software, firmware, and security updates that mitigate risks to consumers and operators. That waiver remains in effect according to its stated terms. Furthermore, the Commission proposes to codify these waivers in its rules.

F. Definition of "Critical Infrastructure" as used in the Covered List

72. In the *EA Security Second Further Notice*, we addressed the U.S. Court of Appeals for the District of Columbia Circuit's partial remand of the Commission's decision in its *EA Security R&O and FNPRM* and sought comment on establishing a new definition of "critical infrastructure" for purposes of our prohibition on authorization of covered equipment produced by Hikvision, Dahua, and Hytera, and their subsidiaries and affiliates.[170] Specifically, the D.C. Circuit vacated those portions of the Commission's decision defining "critical infrastructure" for purposes of understanding when video surveillance and telecommunications equipment produced by Hikvision, Dahua, and Hytera (and their respective subsidiaries and affiliates) is used "for the purpose of . . . physical security surveillance of critical infrastructure," as set forth in section 889(f)(3) of the National Defense Authorization Act (NDAA) of 2019 and incorporated into the Covered List via the Secure Networks Act.[171] The court concluded that the "Commission's choice of reference materials—government sources that define 'critical infrastructure' and related national security concepts—was reasonable, and that the Commission

[170] *EA Security Second Further Notice*, paras. 66-80. We noted that adoption of this definition would be a precondition to the review and approval of any compliance plans, as required under the *EA Security R&O and FNPRM*. *See id.,* para. 73.

[171] *See id.*, para. 66 (citing *Hikvision USA, Inc. v. Federal Communications Commission*, 97 F.4th 938, 948-50 (D.C. Cir. 2024) (*Hikvision*)); *see also* Pub. L. 115-232, § 889, 132 Stat. 1636, 1917-19 (2018) (2019 NDAA § 889); 47 U.S.C. § 1601(c)(3).

adequately explained why the cited sources were relevant."[172] However, the court found that the Commission had failed to explain or justify why the definition should include any "systems or assets" that are merely "connected to" critical infrastructure sectors or functions and that the scope of the definition was "therefore arbitrarily broad."[173] The court vacated those portions of the *EA Security R&O and FNPRM* defining "critical infrastructure," and remanded to the Commission to "comport its definition and justification for it" with the NDAA statutory provision.[174]

73. Today, we retain our reliance on the government sources that the D.C. Circuit upheld, but narrow the definition to no longer interpret "critical infrastructure" to broadly encompass all components "connected to" critical infrastructure. We define "critical infrastructure" per Section 1016(e) of the USA PATRIOT Act of 2001 (Patriot Act) as: "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[175] We further provide guidance noting that this definition encompasses systems and assets used in the provision of services or functions in the 16 critical infrastructure sectors as identified in Presidential Memoranda and elaborated on by the Department of Homeland Security (DHS)[176] to provide any of the 55 National Critical Functions (NCFs) published by DHS through the National Risk Management Center (NRMC).[177] In adopting this definition, we apply the same base definition, taken from the Patriot Act, of "critical infrastructure" that the Commission originally adopted in the *EA Security R&O and FNPRM* that was affirmed by the court, and we provide guidance to facilitate the determination of what is "vital" that follows longstanding presidential and DHS judgments. But we eliminate the "connected to" provision of the *EA Security R&O and FNPRM* that the court found overly broad.[178] In doing so, we make clear that we are not expanding the scope of the Patriot Act definition, but rather are providing additional guidance concerning what systems or assets are "vital" under that definition.

74. Commenters generally agree that the Commission should adopt the Patriot Act definition of "critical infrastructure."[179] In addition to being codified law, the Federal government has consistently used this definition in national policy documents, including Presidential Policy Directive 21 and National

[172] *Hikvision*, 97 F.4th at 949.

[173] *Id.*

[174] *Id.*

[175] 50 U.S.C. § 5195c(e).

[176] National Security Memorandum on Critical Infrastructure Security and Resilience, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (Apr. 30, 2024) (NSM-22). NSM-22 identifies the same sixteen "critical infrastructure sectors" identified in Presidential Policy Directive 21 (PPD-21): chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. *See id.* DHS provides more detail on its website. *See* Cybersecurity & Infrastructure Security Agency, *Critical Infrastructure Sectors*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited June 22, 2026).

[177] *See* Cybersecurity & Infrastructure Security Agency, *National Critical Functions Set*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited June 22, 2026).

[178] *Second Report and Order*, para. 74.

[179] *See, e.g.*, Center for Regulatory Freedom Comments at 7; CTIA Comments at 20-21; Foundation for Defense of Democracies Comments at 2; MEMA Comments at 8; NCTA Comments at 4; USTelecom Comments at 11; CTIA Reply at 16; Motorola Reply at 2-3; NCTA Reply at 8-10.

Security Memorandum 22.[180] We conclude that this definition is consistent with existing precedent and aligns with current Executive Branch policy directives regarding critical infrastructure.

75. Likewise, the definition that we adopt today is consistent with the D.C. Circuit's opinion. In the *EA Security R&O and FNPRM*, the Commission interpreted the prohibition in 2019 NDAA § 889 as having broad scope with respect to Hikvision, Dahua, and Hytera equipment because such equipment poses an unacceptable risk to national security.[181] The court concluded that "[t]he Commission's choice of reference materials—government sources that define 'critical infrastructure' and related national security concepts—was reasonable, and that the Commission adequately explained why the cited sources were relevant."[182] The court noted that even Hikvision conceded that the Commission's application of the Patriot Act definition of critical infrastructure "may be appropriate."[183] We have now made clear that the definition we adopt today no longer encompasses systems and assets that are merely "connected to" the 16 critical infrastructure sectors, which was the main focus of the court's decision.[184] We conclude that continuing to use the Patriot Act definition, in conjunction with the 16 critical infrastructure sectors and the 55 NCFs, is the best course and is responsive to the court's opinion.

76. In the *2d FNPRM*, we sought comment on interpreting "critical infrastructure" as "encompassing equipment when used in the provision of services or functions in the 16 critical infrastructure sectors," even if the equipment is not "so vital to the United States" to be considered "critical infrastructure."[185] Some commenters argue that service providers will face implementation challenges if we include all such equipment within the scope of the definition. In recognition of those concerns, we here decline to encompass all equipment used in the provision of services or functions in the 16 critical infrastructure sectors.[186] We instead provide that the definition adopted today encompasses systems or assets used in the provision of services or functions in the 16 critical infrastructure sectors *when used to provide any of the 55 NCFs*, a distinction that better ensures that the systems and assets in question are reasonably understood as "vital" within the meaning of the Patriot Act definition.

77. We reject Hikvision USA's argument that the proposed definition "does not provide the narrowing or comprehensible guidance required by" the D.C. Circuit and assertions that there is "little or no practical difference between the new proposal and the [original] definition" that the court vacated and remanded to the Commission.[187] Both as proposed in the *2d FNPRM* and as adopted today, our definition of critical infrastructure is different from the definition the Commission adopted in the *EA Security R&O*, which "threaten[en]d to envelop ever-broadening sectors of the economy."[188]

---

[180] *See* Directive on Critical Infrastructure Security and Resilience, 1 Pub. Papers 106, 115 (Feb. 12, 2013) (PPD-21), https://www.govinfo.gov/content/pkg/PPP-2013-book1/pdf/PPP-2013-book1-doc-pg106.pdf; NSM-22.

[181] *First Report and Order*, para. 209.

[182] *Hikvision*, 97 F.4th at 949.

[183] *Id.* at 949.

[184] In *Hikvision*, the court noted that the Commission "does not explain why everything 'connected to' any sector or function that implicates national security must be considered 'critical,' especially in light of the Patriot Act's emphasis on particular 'systems and assets' that are 'vital to the United States.'" *Hikvision*, 97 F.4th at 949-50. The court found that the Commission's definition "threatens to envelop ever-broadening sectors of the economy," and reads the word "critical" out of the statute and applies the equipment ban to all "infrastructure." *Id.* at 950. The court found it "entirely implausible that every single system or asset that is 'connected to,' for example, the food and agriculture sector, or to the function of supplying water, is 'critical' to the national security of the United States," and it noted that the Commission has not identified any relevant infrastructure that would not be covered, whether critical or not. *Id.*

[185] *Second Report and Order*, para. 79.

[186] *Second Report and Order*, para. 79.

[187] Hikvision Comments at 13.

[188] *Hikvision*, 97 F.4th at 950.

Specifically, the definition now includes systems and assets used in the provision of services or functions in the 16 critical infrastructure sectors to provide any of the 55 NCFs, but it does not include all systems and assets merely "connected to" the provision of those services and functions. And we again emphasize that we are explicating, not expanding on, the Patriot Act definition. That is, we interpret critical infrastructure to encompass only systems and assets "so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Systems or assets that are not vital in this way are not encompassed, even if they could conceivably be characterized as being used in the provision of services or functions in the 16 critical infrastructure sectors to provide the 55 NCFs. Moreover, DHS has helpfully provided extensive online guidance as to the content of the 16 critical infrastructure sectors and the 55 NCFs.[189] We follow this guidance. We find the definition we adopt today will reduce implementation challenges by providing sufficient guidance and provide industry stakeholders with the information necessary to fully comply with our rules.

78. We also decline to adopt Hikvision USA's definition of "critical infrastructure."[190] Hikvision USA proposes that the Commission use a finite list of 10 systems and assets—across multiple sectors—to define the bounds of critical infrastructure.[191] It argues that it is enough to include only those specific systems and assets (governmental and private)—which are, in their view, "so vital to the United States that individually incapacitating or destroying those systems and assets would have a debilitating impact on national security, national economic security, and/or national public health or safety."[192] We conclude that Hikvision USA's proposed definition is not consistent with the Patriot Act definition, excluding several systems and assets that, if incapacitated or destroyed, would result in "a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[193] These include systems and assets used in communications, critical manufacturing, emergency services, food and agriculture, and healthcare and public health—sectors recognized in PPD-21 and reaffirmed in NSM-22, and by DHS, as critical infrastructure sectors. We reject Hikvision USA's arguments, which are contrary to a presidential determination and years of U.S. government policy, that not all of the 16 critical infrastructure sectors are "vital" to the security of the United States within the meaning of the Patriot Act.[194] For example, the Department of Agriculture's National Farm Security Action Plan notes the food and agriculture sector is "a known target for terrorists and malicious actors" requiring that the U.S. government "elevate it to the top echelon of national security priorities."[195] Hikvision USA's arguments ignore the interconnected nature of our communications networks that are essential to the successful operation of the 16 critical infrastructure sectors and also are contrary to the broad definition we find necessary in implementing the 2019 NDAA Section 889.[196] And again, the D.C. Circuit already found that the Commission's reliance on the 16 critical infrastructure sections was

[189] *See* Cybersecurity & Infrastructure Security Agency, *Critical Infrastructure Sectors*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited June 23, 2026); Cybersecurity & Infrastructure Security Agency, *National Critical Functions Set*, https://perma.cc/YGK2-YQU2 (last visited June 24, 2026).

[190] *See* Hikvision Comments at 19-22 (citing Compliance Plan of Hikvision USA, Inc., ET Docket No. 21-232, at 7 (filed Apr. 29, 2024), https://www.fcc.gov/ecfs/document/10429064727762/2 (April Compliance Plan)).

[191] *See id*.; Hikvision Comments at 20.

[192] *See* April Compliance Plan, at 7.

[193] *Second Report and Order*, para. 80.

[194] *See* Hikvision Comments at 21.

[195] Department of Agriculture, National Farm Security Action Plan, https://www.usda.gov/sites/default/files/documents/farm-security-nat-sec.pdf (last visited June 22, 2026).

[196] *See EA Security Second Further Notice*, para. 80 (citing *EA Security R&O*, 37 FCC Rcd at 13576-77, paras. 208-09).

reasonable and reasonably explained.[197] In short, we conclude that the best definition of the statutory term "critical infrastructure" as found in Section 889 is to adopt the Patriot Act definition, explicated by the services or functions in the 16 critical infrastructure sectors and the 55 NCFs.

G. Rule Correction and Clarification

79. In the *Second Report and Order*, we redesignated former paragraphs (b) through (d) of Section 2.903 as paragraphs (d) through (f). Cross-references within paragraphs (d)(1) through (d)(3) inadvertently retained references to former paragraph (b) instead of the newly redesignated paragraph (d). We correct that scrivener's error today.

80. We also adopt corrections to administrative errors in section 2.1204(a) of the Commission's rules. In section 2.1204(a)(2), we are adding the word "and" which was missing between "technical" and "administrative[.]" Finally, we delete section 2.1204(a)(4)(iv), because it is a duplicate of 2.1204(a)(4)(iii), which immediately precedes that section.

H. Regulatory Impact Analysis

1. Need for regulatory action

81. Regulatory action is necessary because the current equipment authorization framework contains unresolved vulnerabilities that adversarial actors can continue to exploit, particularly through high-risk components, opaque supply-chain pathways, and permissive marketing or modification practices. If we leave these vulnerabilities unaddressed, Covered List entities will remain capable of inserting malicious firmware, intercepting sensitive information, or compromising communications networks through components such as logic-bearing hardware components, even when embedded within otherwise authorized devices. Without targeted updates to the authorization, marketing, and enforcement rules, these gaps would persist and could expose U.S. communications infrastructure and consumers to unacceptable national-security risks. At the same time, the rule changes under consideration are designed to be narrowly tailored to specific, well-supported national-security determinations, ensuring that the Commission strengthens protections while avoiding unnecessary disruption to lawful supply chains. Taken together, these factors demonstrate that regulatory action is required to safeguard U.S. telecommunications networks and the public interest in a balanced, risk-minimizing manner.

82. This significant regulatory action is submitted to the Office of Information and Regulatory Affairs (OIRA) for interagency review. This regulatory impact analysis (RIA) presents an assessment of the costs and benefits, including regulatory compliance costs, associated with this action and is consistent with Executive Order 12866. Comparing the proposed rules with other alternative policy options, we find that the adoption of these proposed rules will result in significant benefits that outweigh the associated costs. This rule is not an Executive Order 14192 regulatory action because it is being issued with respect to a national security function of the United States.

2. Benefits

83. The rules adopted in the *Third Report and Order* that take security into consideration in the equipment authorization process would serve the public interest by addressing significant national security risks that have been identified by the Commission, and by Congress and other federal agencies, and would be consistent with the Commission's broad statutory authority. The Commission finds that extending the prohibition to include logic-bearing hardware components produced by named and identified entities on the Covered List is necessary to close the existing gap in equipment posing unacceptable risks to national security. These components, similar to previously banned modular transmitters, are integral to the operation of American communications networks, but they can be leveraged by foreign adversaries for surveillance, monitoring, and malicious interference. The Commission's prior analysis has established that adversary access to network infrastructure, whether through transmitters or other critical modules, presents a consistent risk and enables exploitation for

[197] *Hikvision USA, Inc v. FCC, 97 F.4th 938 (2024)*.

unauthorized data collection and disruption of essential services.

84. Logic-bearing hardware components—when sourced from named and identified entities on the Covered List—may facilitate covert surveillance, network disruption, and unauthorized access to confidential information. The economic impact of such threats is profound. In 2025, the national GDP exceeded $30 trillion,[198] and even a modest disruption or breach could result in losses amounting to billions of dollars, undermining public confidence and economic stability. The Commission estimates that preventing even one percent of malicious cyber activity or network disruption would yield direct economic benefits in the hundreds of millions,[199] far outweighing the modest costs associated with enhanced security requirements adopted by this *Order*.

85. These rules are intended to eliminate ambiguity in our marketing and enforcement framework and to further close loopholes that have allowed unauthorized or covered equipment to reach U.S. consumers and networks. As clarified in this *Order*, activities undertaken by online marketplaces—such as listing regulated devices online, engaging in consignment or warehousing arrangements, performing order processing, labeling, packaging, billing, and other fulfillment services—constitute "distribution for the purpose of selling" and therefore fall within the scope of our marketing rules. These clarifications align our interpretation with analogous federal consumer protection practices and ensure that downstream entities with meaningful involvement in the sale and placement of RF equipment into U.S. commerce cannot evade accountability. Together with our decision to require online marketplaces to display FCC IDs at the online point of sale, these measures strengthen the Commission's ability to intercept unauthorized devices before they enter the marketplace, bolster consumer transparency, and support the Commission in identifying and removing unlawful or security risk equipment.

86. Additionally, our enforcement and equipment authorization clarifications close gaps that have historically hindered our oversight of foreign manufacturers and Covered List entities. Our clarification that modifications may not be used to reintroduce covered or potentially covered equipment into the supply chain reinforces the Secure Equipment Act's prohibition on authorizing insecure devices. And by requiring Covered List entities to submit full recertification applications for any modification, regardless of scope or authorization pathway, we close a critical loophole that otherwise could allow post authorization tampering or incremental changes to circumvent our national security protections. Collectively, these rule, revisions and clarifications fortify the equipment authorization system, protect U.S. networks from unacceptable risk, and ensure that every actor in the supply chain bears appropriate responsibility for safeguarding the integrity of the communications ecosystem.

87. The Commission concludes that the adopted security measures are justified by the substantial public safety and economic benefits. Safeguarding the integrity of communications networks advances national security and preserves the economic interests of the United States. The Commission affirms that the action is a critical step in mitigating risks, ensuring the continued trustworthiness of network infrastructure, and protecting the interests of American consumers and businesses.

3. Costs

88. We estimate that the actions adopted today will impose costs of approximately $50 million annually.

89. For logic-bearing hardware components, the Commission finds that the domestic market

[198] U.S. Bureau of Economic Analysis, *Table 1.1.5. Gross Domestic Product*, https://apps.bea.gov/iTable/?reqid=19&step=3&isuri=1&categories=survey&nipa_table_list=5&Series=A&select_all_years=1&_gl=1*16zt8m*_ga*MjY2NzAxMjE1LjE3NzUwNzA3ODk.*_ga_J4698JNNFT*czE3NzUwNzA3ODkkbzEkZzEkdDE3NzUwNzA5ODkkajE3JGwwJGgw (last visited May 11, 2026).

[199] The Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy at 36 (Feb. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (estimating the cost of malicious cyber activity on the U.S. economy in 2016 was between $57 billion and $109 billion).

share associated with Covered List entities is comparatively small, and that many U.S. manufacturers have already shifted sourcing away from questionable suppliers due to existing federal procurement restrictions, private-sector risk-management practices, and multi-sourcing strategies implemented over the past several years.[200] Most compliance costs under the *Report and Order* therefore stem from potential product redesigns or component substitution for a narrow subset of firms that still incorporate components from Covered List entities. Because the adopted requirements apply only to future equipment authorizations, and because the responsible-party obligation aligns with compliance procedures already familiar to manufacturers and importers, the Commission expects any redesign or retesting burdens to fall on a limited group of market participants, but it is unclear at this point which market participants would need to conduct redesign and retesting. Accordingly, the operational impacts of these rules are expected to be marginal, and unlikely to generate significant disruptions in ongoing production or supply-chain planning.

90. *Marketing*. The Commission's clarification of its marketing rules, expressly confirming that a carrier's transport of unauthorized devices does not constitute marketing, directly addresses and alleviates the concerns raised by commenters who cautioned against overreach. At the same time, the Commission reaffirms that the prohibition on marketing covered equipment appropriately extends to the listing of regulated devices on an online marketplace when accompanied by activities such as consignment, warehousing, inventory management, order processing, labelling, packaging, billing, or fulfillment services, even where a third-party seller holds title. This clarification is essential to prevent entities from exploiting distribution via online platforms to evade the Secure Equipment Act, and is fully consistent with the marketing rules adopted in the *First* and *Second Report and Orders*. Because these clarifications primarily codify interpretations already embedded in existing rules and enforcement practices, they are not expected to impose additional costs beyond those in prior Commission decisions. The Commission finds that requiring online platforms to display FCC IDs imposes minimal cost burden. Online marketplaces already post comprehensive product information, and adding a single identifier does not increase marginal effort or expense

91. *Enforcement*. We find that assigning the liable-party obligation to the U.S. importers for foreign-manufactured certified equipment will impose minimally incremental burden.[201] Specifically, every device imported into the United States necessarily enters through a U.S.-based importer, which already performs core functions parallel to those required of a liable party—such as maintaining import records, coordinating shipment and distribution, and interacting with federal agencies when compliance issues arise. Because these entities already stand in the supply chain as the domestic point of entry, designating the importer as the liable party does not introduce a new compliance role so much as formalize duties that importers commonly perform today. We conclude that the resulting additional administrative and documentation obligations on U.S. importers are minimal.

92. *Modification and Re-Certification*. The Commission's clarification regarding

[200] *See e.g.*, Markets and Markets, *Optical Transceiver Companies – Coherent Corp. (US) and INNOLIGHT (China) Are the Key Players*, https://www.marketsandmarkets.com/ResearchInsight/optical-transceiver-market.asp (last visited May 15, 2026) (listing the key players in the optical transceiver market, none of which appear on the Covered List); *See* OpporTimes, Top 10 Exporters of Semiconductor Chips to the United States (Aug. 6, 2025), https://www.opportimes.com/en/top-10-exporters-of-semiconductor-chips-to-the-united-states/ (indicating that China comprises a relatively small share of semiconductor chip exports to the United States).

[201] Under § 2.909(a), the "responsible party" for certified equipment is the single party to whom the grant of certification is issued and who bears responsibility for the equipment's compliance with applicable technical and administrative requirements. By contrast, the "liable party" is the U.S.-based party that, by virtue of its designation, is jointly and severally liable with the applicant or grantee for the compliance of FCC-certified equipment. Whereas § 2.909 generally vests compliance responsibility in a single party at any given time (subject to transfer upon modification, contractual assumption, or change of control), the "liable party" designation creates a domestic point of legal accountability that exists alongside, and shares liability with, the applicant or grantee rather than displacing them.

modification and recertification requirements for Covered List entities is necessary to prevent any modification—whether through design changes, production shifts, or permissive software or hardware updates—from transforming previously authorized equipment into covered equipment in violation of the Secure Equipment Act. Prior orders already prohibited authorization of equipment that is, or would become, covered, but ambiguity remained around how these prohibitions applied to permissive changes and post-authorization modifications. Codifying these clarifications ensures that no entity on the Covered List can use incremental updates, redesigns, or changes in production origin to reintroduce national-security risks into the equipment authorization system or circumvent the regulation. By requiring recertification for any modification made by a Covered List entity and affirming that SDoC pathways are unavailable to such entities, the Commission closes loopholes that could otherwise allow covered equipment to be altered in ways that introduce new vulnerabilities. These clarifications resolve prior uncertainty, align implementation with the Secure Equipment Act's directive that the Commission may not review or approve applications for covered equipment. By aligning the rules with the Secure Equipment Act and clarifying their application, the Commission strengthens supply-chain security while reducing costs from ambiguity.

4. Alternate Policies

a. Alternative A – No Action

93. Under this alternative, the Commission would decline to adopt any new measures to address the persistent vulnerabilities identified in the record. This approach would preserve the status quo and impose zero additional implementation costs on regulated entities. Because no new compliance obligations, reporting requirements, or equipment authorization reforms would be introduced, industry would not incur incremental expenditures, redesign costs, or administrative burdens. From a narrow cost accounting perspective, this alternative presents the least immediate regulatory cost impact.

94. However, maintaining the current regulatory framework would leave unaddressed the security gaps and systemic vulnerabilities that have been repeatedly identified across recent national security determinations, including risks associated with logic-bearing hardware components. These gaps are precisely the channels adversarial nation-states can exploit to facilitate intrusion, unauthorized surveillance, data exfiltration, network disruption, and covert access into U.S. communications infrastructure.

95. While it is difficult to estimate the incremental increase in risk of not adopting these rules, as noted above, even a single compromise of network infrastructure can result in cascading economic losses, including service disruptions, theft of sensitive commercial or governmental information, and degradation of critical infrastructure reliability. With the national GDP exceeding $30 trillion in 2025, the Commission has already found that preventing only one percent of malicious cyber activity or communications disruption would yield benefits in the hundreds of millions of dollars. Under this noaction alternative, those risks would remain unmitigated, exposing U.S. consumers, businesses, and government systems to continued and potentially escalating threats.

96. Therefore, although this alternative appears cost neutral from an implementation standpoint, it carries substantial hidden costs in the form of heightened exposure to national security threats. The Commission finds that the economic and national security risks associated with preserving the status quo could easily result in harm costing hundreds of millions of dollars, far exceeding any near-term administrative savings.

b. Alternative B – Adopt Rules with Broad Ban on All Components Produced by Named and identified entities on the Covered List

97. Under this alternative, the Commission would impose a broad prohibition on all components produced by Covered List entities, including hardware, firmware, and software, regardless of their specific role or relevance to any particular national security determination. Although such an approach might appear comprehensive, it would create significant and widespread burdens for manufacturers and downstream supply chain participants and could lead to increased prices and possible

equipment shortages.

98. A universal component ban would require industry to trace the origin of thousands of inputs that flow through complex global supply chains. This would far exceed the targeted, risk based prohibitions adopted in the *Third Report and Order* for specific component classes such as logic-bearing hardware components, which were supported by detailed findings in the record. A broad ban would likely force extensive redesigns of many products, require retesting to maintain compliance, and disrupt well established sourcing arrangements, particularly for smaller firms with limited supply chain flexibility.

99. These disruptions could translate into substantial consumer harms. Manufacturers facing higher procurement and redesign costs would pass these costs on to consumers in the form of higher prices, reduced product availability, and slower deployment of new technologies. Shortages or delays in critical communications equipment could also impair broadband deployment, IoT adoption, and upgrades essential to national competitiveness.

100. Finally, expanding restrictions without clear risk based justification would impose economic costs that are disproportionate to any incremental security benefits. For these reasons, although the broad ban would reduce theoretical exposure to Covered List components, it would also cause major supply chain disruption, increase costs across the communications sector, and result in substantial consumer harms that outweigh the potential benefits of this alternative.

c. Alternative C – the Adopted Rules

101. This alternative, which we adopt, is a targeted set of rules designed to close specific national-security gaps while avoiding unnecessary disruption to manufacturers, supply chains, or consumers. The adopted approach focuses on components and practices that the record shows present the greatest national security risks, including logic-bearing hardware components produced by named and identified entities on the Covered List, rather than applying a blanket prohibition across all components. This ensures that Commission action remains tightly aligned with clear national-security determinations, consistent with statutory requirements.

102. By limiting prohibitions to components directly implicated in national security findings, this alternative minimizes operational and redesign burdens on industry. The record demonstrates that most suppliers in these categories already rely heavily on trusted manufacturers, and that only a small fraction of the market is affected by these targeted restrictions. As a result, the expected cost impacts are modest, and the changes apply only to future equipment authorizations, allowing continued use of previously authorized equipment during a transition period.

103. This balanced approach also reduces potential downstream harms to consumers. By avoiding the broad, sweeping restrictions contemplated under Alternative B, the adopted rules help preserve product availability, maintain price stability, and prevent disruptions to critical communications deployments. At the same time, they strengthen oversight of high risk components, reinforce marketing and enforcement safeguards, and improve supply chain accountability in a manner proportionate to the threats identified.

104. For these reasons, the Commission finds that this alternative offers an effective framework that meaningfully addresses national security risks while limiting unnecessary economic burdens. The adopted rules strike an appropriate balance: they close known vulnerabilities, enhance the security of U.S. communications networks, and protect the public interest, all while minimizing impacts on the supply chain and reducing potential consumer harm.

5. Justification Determination

a. Benefits Exceed Costs

105. We find that the changes being adopted in the *Third Report and Order* should generate substantial benefits to national security and the resiliency of critical communications infrastructure, and

that these benefits far outweigh the moderate compliance costs. The benefits of enhanced protection of U.S. communications networks are substantial, but are difficult to quantify. We find, however, that the adopted actions are expected to have an annual effect on the economy of $100 million or more in benefits. In contrast, we estimate annual costs of approximate $50 million for the removal of cellular IoT modules. We find that the costs of removing logic-bearing hardware components produced by named and identified entities on the Covered List to be negligible because of the limited markets shares of such entities in the United States in these product categories. Therefore, we find that the benefits of strengthening oversight and protecting communications networks significantly outweigh the costs.

Table of Benefits and Costs

	Recurring (per year)	Present Value over 5 Years (3% discount)	Present Value over 5 Years (7% discount)
Benefits			
Quantitative	N/A	N/A	N/A
Qualitative	The Commission views this item as economically significant based on the benefits, i.e., having annual benefits exceeding $100 million.		
Costs ($millions)	$50	$236	$219

b. Highest Net-Benefit Alternative

106. Based on the record and economic analysis, Staff find that Alternative C offers the greatest net benefit among the three alternatives considered. The adopted rules bolster national security with respect to our nation's equipment authorization system, coupled with targeted measures to limit burdens on the supply chain and consumer welfare. Alternative A is inferior because of the unacceptable national security risks that lack of action entails. Alternative B is inferior to Alternative C because it could result in significantly higher compliance costs without commensurate improvements in national security.

IV. THIRD FURTHER NOTICE OF PROPOSED RULEMAKING

107. In this *Third Further Notice of Proposed Rulemaking* we identify several additional loopholes in the current regulatory framework that may create vulnerabilities with potential implications for national security. We propose targeted rules to close these gaps and prevent entities from exploiting ambiguities that undermine the Commission's safeguards. We find that these measures would further strengthen the security and integrity of the nation's communications networks and yield substantial benefits for national, economic, and public security. We also seek comment on measures to strengthen enforcement by requiring a U.S.-based liable party for FCC-certified equipment. We also propose and seek comment on a wide range of additional measures that will modernize our Covered List rules, given recent updates to the Covered List that identify covered equipment based on production location. These include updates to Parts 2 and 15 of our rules concerning the Covered List; white-labelling; hardware and software bills of materials; further prohibitions or presumptions against authorization of equipment containing Covered List components or software; certification requirements for devices in Covered List sectors; equipment importation rules (including the importation for personal use and related definitions in Part 15); equipment marketing rules (including prohibitions on marketing and use for illegal or unlawful purposes and related definitions in Part 15); use of the FCC logo; streamlined revocation proceedings; codifying previously granted and expanded waivers permitting permissive changes; operating devices prior to authorization; UAS and router Covered List definitions; term limits on equipment authorizations; registration of SDoC devices; data analytics capability and need for modern EAS database; submarine cables; and a U.S.-based liable party requirement for FCC-certified equipment.

A. Bifurcating Covered List rules

108. In light of recent updates to the Covered List consisting of production location-based Covered List entries applying to specific sectors of devices (i.e. UAS, UAS critical components, and routers),[202] the Commission seeks comment on a series of rules changes that would, in effect, bifurcate the Covered List into producer/provider-based and production location-based categories to provide clarity for compliance. Some rules must necessarily apply to both categories—for example, the statutory requirement that the Commission prohibit the authorization of equipment on the Covered List.[203] But some of the Commission's existing rules only apply to the first category. As noted above,[204] rules applying to devices "produced by an entity identified on the Covered List" necessarily only apply to the first category, as they are predicated on the existence of a *producer*. The Commission now seeks comment on establishing some rules that apply only to the second category of covered equipment, production location-based covered equipment. Additionally, the Commission seeks comment on some rules changes that would apply to devices within a sector subject to a production location-based Covered List entry (i.e. UAS, UAS critical components, routers, and any sector subject to analogous specific determinations). We refer to these as devices in a "Covered List sector." To that end, we propose to reorganize our Part 2 rules and to direct PSHSB (which maintains the Covered List website) to redesign the website into 2 columns to reflect this proposed bifurcation.

B. White Labeling

109. In the *First Report and Order*, the Commission expressed concern regarding the authorization of privately labeled, rebranded, or relabeled ("white labeled") covered equipment and made clear that white labeling of any covered equipment does not change the status of whether the equipment is covered equipment.[205] We seek comment on how and whether the phrase "produced by" in specific determinations as reflected on the Covered List should be interpreted, in a manner consistent with the Secure Networks Act and the various specific determinations,[206] to address these concerns.

110. In the *Second Report and Order*, the Commission clarified that, in interpreting whether equipment is "produced by" a specific entity identified on the Covered List, applicants, responsible parties, and entities named in their reporting obligations should take a broad view of the term 'produced by.'"[207] We declined at that time to adopt a comprehensive definition of "produced by," but the Commission did offer some general guidance that "produced by" "likely includes substantial responsibility for or control over any major stage of the process by which a device comes into existence," multiple entities could be said to have produced a single device, and that "produced by" would generally include the design, manufacturing, assembly, or development of the device.[208] However, we also noted, in response to an *ex parte* comment from Eagle Electronics, a U.S. module company, that we did not intend to suggest that we "consider originating design IP as a sole factor in determining whether a device

[202] *See* Federal Communications Commission, List of Equipment and Services Covered by Section 2 of the Secure Networks Act ("Covered List"), https://www.fcc.gov/supplychain/coveredlist, (Last visited June 26, 2026).

[203] *See* 47 CFR § 2.903(a).

[204] *See supra*, para. 66.

[205] *First Report and Order, paras. 187-88.*

[206] Such specific determinations include the determinations by Congress in the 2019 NDAA as to "[t]elecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities)" and "video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities)," *see* Pub. L. 115-232, § 889, 132 Stat. 1636, 1917-19 (2018) (2019 NDAA § 889), as well as any subsequent determinations that have been or may be made using the phrase "produced by" that we determine to be specific determinations triggering 47 U.S.C. § 1601(c).

[207] *Second Report and Order*, para. 53.

[208] *Second Report and Order,* para. 53.

is produced by a particular entity."[209]

111. Eagle Electronics contends that if an item is "produced by" a foreign entity based on its design, in particular "solely due to originating design IP" then that "would also prevent American companies from reshoring vital technology even if they can redevelop, secure, and improve the product, manufacturing a new and distinct product that is solely under U.S. control."[210] Eagle Electronics suggests that this could undermine American national security. For that reason, Eagle Electronics suggested that any definition of "produced by" should exclude cases where "a U.S. liable party (i) exercises exclusive design control and exclusive authority over compilation, cryptographic signing, and delivery of firmware/updates for the device's logic-bearing subsystems, (ii) precludes any third-party update pathway through secure-boot/cryptographic binding, and (iii) provides independent security evaluation and supply-chain provenance."[211]

112. By contrast, Telit Cinterion, another module producer, commented on the *Second Further Notice*, encouraging the Commission to codify a more expansive definition that would that "include[] any entity that designs, develops, manufactures, supplies, signs firmware, controls over-the-air update infrastructure, manages eSIM/subscription provisioning, or holds cryptographic keys/certificates for an RF module or device, regardless of brand, reseller, or licensee arrangements."[212]

113. Now, the Commission seeks comment on whether to codify a definition of "produced by" for purposes of the Covered List and related Commission rules.[213] We seek comment on whether the Commission should formally codify in our rules that: "A device is 'produced by' an entity if that entity exercises substantial responsibility for, or control over, any major stage of the process by which the device comes into existence, including the design, manufacturing, assembly, or development of the device. A device may be 'produced by' more than one entity." If the Commission codifies this definition, should the Commission, as recommended by Eagle, expressly exclude cases in which an entity is solely responsible for the originating design IP but a U.S. liable party (i) exercises exclusive design control and exclusive authority over compilation, cryptographic signing, and delivery of firmware/updates for the device's logic-bearing subsystems, (ii) precludes any third-party update pathway through secure-boot/cryptographic binding, and (iii) provides independent security evaluation and supply-chain provenance? Alternatively, should the Commission adopt a different definition? Should we adopt a narrower definition, perhaps excluding design entirely? Should the Commission instead adopt a broader definition? For example, should the Commission adopt the definition that Telit Cinterion proposes?

114. Currently, applicants seeking equipment authorization must certify, among other things, that the equipment for which authorization is sought is not prohibited from receiving equipment authorization as covered equipment and "[a]n affirmative or negative statement as to whether the applicant is identified on the Covered List."[214] Is this sufficient to prevent white labeling of covered equipment? The Commission seeks comment on whether to adopt a requirement that an applicant for equipment authorization provide a written and signed list of any and all entities that produced the device for which equipment authorization is sought. Would this better allow the Commission to ensure that white-labelled covered equipment does not inadvertently receive equipment authorization? Specifically, how might this help the Commission monitor devices for which there is more than one producer, one of which is an entity identified on the Covered List? What are the costs and benefits of such a requirement?

---

[209] *Second Report and Order,* para. 53, n. 205.

[210] Letter from Mark Kvamme, Chairman and Matt Wyckhouse, Board Member, Eagle Electronics, to: Marlene Dortch, Secretary, Federal Communications Commission, Docket No. 21-232, at 3. Filed October, 15, 2025.

[211] *Id*.

[212] Telit Cinterion Comment at 6.

[213] *See, e.g.*, 47 CFR §§ 2.906(d), 2.938(b)(2), 15.103(j).

[214] 47 CFR § 2.911(d)(5).

115. The Commission further seeks comment on whether white labelers seeking equipment authorizations have abused, or could abuse, our rules streamlining certification requirements for devices claiming "electrically identical" status. We seek comment on proposals to address the potential for abuse. The Commission's rules permit a grantee, or under authorization of the grantee, to market a device that is "electrically identical" to an authorized device without obtaining a new certification or SDoC authorization, and electrically identical devices may share the same FCC ID even though marketed under different model numbers.[215] Electrically identical devices share the same exact internal electrical circuitry, RF characteristics, and emissions profiles, but can be marketed under different model names or trade names under the same FCC ID. Our rules also permit a change in identification procedure, where another company can white-label an existing, certified product "without a change in design, circuitry or construction" and legally sell it under their own brand name with their own FCC ID without resubmitting equipment or measurement or test data.[216] In our experience, entities have abused this procedure to evade our enforcement authority.[217]

116. Typically, the Commission receives notice of electrically identical equipment either through test measurement reports that are filed as part of the original application for certification or through a subsequent filing in which the grantee identifies specific trade models and avers that they are electrically identical to the unit that was originally tested and found to be compliant. Entities that wish to rebrand or white label an authorized device may, with permission of the grantee, market an electrically identical version using the grantee's original FCC ID. [218] This type of white labeling arrangement should be, but might not always be, captured within the equipment application files for both entities in our EAS database. However, white label entities may also apply for their own certification and market the device under their own unique FCC ID; in such cases, the Commission receives no statement that links the original grantee to one or more white label grantees. To the extent that one of several electrically identical devices, marketed under different brands and trade models, is later found to be noncompliant or pose a potential security risk, there is no current means to swiftly identify the remaining electrically identical trade models, which may present the same risks.

117. We seek comment on the extent to which manufacturers or providers engage in the production of white-labeled RF devices for the U.S. market,[219] and we seek comment on a range of other measures the Commission could adopt to address potential white labeling. Does a similar white label market exist for components, such as IoT modules or UAS critical components, that could be produced for the service and repair industry? Given the lack of transparency concerning white labeling arrangements, should we require equipment authorization applicants to disclose all known "electrically

[215] *See, e.g.,* 47 CFR §§ 2.924, 2.933.

[216] 47 CFR § 2.933.

[217] In February 2024, security researchers publicly disclosed security vulnerabilities in Eken-branded doorbell cameras that allowed hackers to view private home video streams, and an FCC commissioner publicly investigated the incident. *See* Starks Letters to Amazon, Sears, Shein, Temu, and Walmart (Mar. 8, 2024), https://www.fcc.gov/document/starks-letters-amazon-sears-shein-temu-and-walmart. Twelve days later, a new grantee, Converge Beauty, obtained different FCC IDs for doorbell cameras "electrically identical" to Eken equipment; Converge Beauty did not need to submit new test reports. *See* https://fcc.report/FCC-ID/2BFEP-M50/7188075.pdf. Converge Beauty's filing was signed by Eken employees. Eken failed to respond to the Commission's initial attempts to investigate in 2024, leading the Commission to issue a Notice of Apparent Liability later that year. *Eken Group Limited*, Notice of Liability for Forfeiture, FCC 24-122, 39 FCC Rcd 12990 (2024) (proposing $730,000 statutory maximum civil penalty against a foreign doorbell camera manufacturer for submitting false certifications under section 2.911(d) regarding its U.S. agent for service of process).

[218] 47 CFR § 2.933.

[219] *See, e.g., These Video Doorbells Have Terrible Security. Amazon Sells Them Anyway*, Consumer Reports (Feb. 29, 2024), https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/ (identifying seemingly identical video cameras, controlled by same app, sold under brand names Eken, Tuck, Fishbot, Rakeblue and others).

identical" products? For instance, if a device has been authorized and the liable party then licenses or authorizes an applicant or another entity to produce an electrically identical device, should the liable party be required to disclose that entity, brand name, and device model? To the extent that the Commission does not adopt a requirement to provide complete HBOM and SBOM, should applicants still be required to provide the origin of the device, i.e., where its components were produced? Should applicants update the Commission whenever new "electrically identical" products are imported or marketed? Should the Commission limit the ability to market "electrically identical" products under section 2.924 without a separate authorization? Should the Commission limit the grantee's ability to change identification of "electrically identical" products under section 2.933? Should the Commission adopt any other counter-white labeling measures?

C. Hardware and Software Bill of Materials

118. The Commission's equipment authorization rules have, until recently, focused principally on the finished device — whether the equipment as a whole is produced by an entity identified on the Covered List and whether it complies with applicable technical standards. In this proceeding, however, the Commission's inquiry has increasingly turned to the component parts from which equipment is assembled. In the *Second Report and Order*, the Commission prohibited the authorization of devices containing covered modular transmitters, and in the *Third Report and Order* above, the Commission extends that approach to devices containing logic-bearing hardware components produced by Covered List entities.[220] This shift reflects a recognition that the national security risks a device poses may be determined as much by the provenance of the components embedded within it, as its outward branding or even final assembly. The recent production location-based additions to the Covered List—covering UAS, UAS critical components, and routers produced in a foreign country—sharpen this concern. Unlike producer/provider-based determinations, which turn on the identity of a known entity, production location-based determinations turn on *where* and *how* a device or its components are made. The addition of UAS critical components, in particular, demonstrates national security agencies' concern with device components.

119. Applying such determinations requires information that has not traditionally been seen as relevant to equipment authorization: the geographic origin of components, the location of design and development activity, and the composition of a device's supply chain. The Commission's existing certification record, which centers on technical compliance and a small set of attestations, was not designed to capture this information. At the same time, the Commission's experience implementing its Covered List rules—and the broader experience of its federal partners—underscores that supply-chain monitoring is now central, rather than ancillary, to the equipment authorization program's national-security function.[221] Against this background, the Commission seeks comment on whether SBOM and HBOM disclosures, together with producer and origin reporting, would give the Commission, TCBs, and other stakeholders the visibility into component-level provenance that the current rules do not provide, but are necessary to fulfilling our obligations under the Secure Networks Act, Secure Equipment Act, and our related rules.

120. As noted by Somos, Inc., the use of SBOM and HBOM to provide transparency is common in modern software supply-chain risk management practices.[222] For consumers of electronics,

[220] *Second Report and Order,* 40 FCC Rcd at 8436-46, paras. 14-31; supra, para. 14-35.

[221] Additionally, the President's National Security Strategy (NSS) states that "the United States must never be dependent on any outside power for core components." National Security Strategy at 13. The NSS further notes that "the Intelligence Community will monitor key supply chains and technological advances around the world to ensure we understand and mitigate vulnerabilities and threats to American security and prosperity." *Id*.

[222] Somos, Inc at 6*; see also* Lucas Tate, et al., *Comparing Bills of Material,* Pacific Northwest National Laboratory (2024), https://arxiv.org/pdf/2411.10384 ("Recently, BOMs have been gaining traction as a tool to increase our supply chain understanding and help respond to this threat."); Seth Carmody, et al., *Building resilient medical technology supply chains with a software bill of materials,* npj Digit. Med. 4, 34 (2021),

(continued….)

SBOM and HBOM play a similar role that ingredients labels play for consumers of food and drug products; they provide transparency about what is found inside a regulated good. Many manufacturers already develop such materials to satisfy existing standards.[223] We seek comment on requiring that applicants for equipment authorization submit a written and signed HBOM and SBOM at the time they apply for certification and requiring that grantees update the Commission of any changes to the HBOM or SBOM of the device. Under the proposed requirement, all components of a device, including hardware, software, and firmware would be subject to disclosure. The disclosure would be required to identify: the producer of each component, the location of each component's production, and the percentage of component value associated with each production location. For example, if all components were manufactured in the U.S., the location value would be 100 percent assembled in the U.S. If production occurs in multiple locations, the disclosure would identify each country involved and the corresponding percentage of component value (e.g., XX percent manufactured in Country A, XX percent manufactured in Country B). If an equipment authorization is granted, the grantee would be required to update the HBOM and SBOM submissions within 30 days of any changes therein.

121. The Commission seeks comment on this approach broadly. What are the costs and benefits of such a proposal? Could such a proposal better ensure that the Commission can better monitor the equipment authorization process to ensure that covered equipment does not get authorized? Would such a proposal help better inform consumers regarding the devices they purchase? What are the burdens on industry that would be associated with this proposal? We observe that a wide range of free and open-source SBOM generation tools are already broadly available and widely used across the software development ecosystem.[224] We tentatively conclude that the burden associated with producing SBOMs for newly developed software using automated methods is negligible. We seek comment on this tentative conclusion. We also seek comment on the costs of implementing SBOM requirements for existing software products. Specifically, we estimate these costs to be under $5,000 per software program. We further estimate the HBOM requirements may cost up to $10,000 in engineering input and information gathering per hardware equipment. We estimate approximately 50% of equipment seeking authorization by the Commission has already met the proposed SBOM and HBOM requirements. We seek comment with specific quantitative evidence on whether these estimates are reasonable, too high, or too low, and whether alternative cost estimates or methodologies should be considered.

122. Alternatively, should the Commission limit the HBOM and SBOM requirements to equipment authorizations for devices in a Covered List sector? In other words, should we only require HBOM and SBOM submissions for devices that are UAS, UAS critical components, or routers[225] (as well as any future Covered List sector)? These are sectors where Commission oversight is most critical to

https://doi.org/10.1038/s41746-021-00403-w ("An example of effective application of the SBOM concept comes from the financial services industry. By 2015, a series of software supply-chain vulnerabilities had forced the industry to re-evaluate the third-party software in its infrastructure. This sector quickly adopted SBOM concepts into their internal development and procurement processes. Now, if a vendor can provide an SBOM, it serves as a litmus test for the maturity of the vendor's organization. If vendors lack an SBOM, many financial services organizations anticipate that their products will likely cost more to evaluate, operate, and own over their lifecycles. As a result, the financial organizations might negotiate discounts to account for these increased costs.").

[223] For example, the Food and Drug Administration (FDA) now requires that manufacturers of FDA-regulated cyber devices provide an SBOM for the commercial, open-source, and off-the-shelf software components contained within the device. *See* Food and Drug Administration (FDA), *Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)*, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs. (Last visited June 26, 2026).

[224] Widely available open-source tools include Syft, Microsoft SBOM tool, CycloneDX generator, SPDX SBOM generator, Wiz. *See* Wiz.com, *Guide to SBOM Tools: 5 Picks for Enterprise Security Teams,* May 6, 2026, https://www.wiz.io/academy/application-security/top-open-source-sbom-tools.

[225] *See* Federal Communications Commission, List of Equipment and Services Covered by Section 2 of the Secure Networks Act ("Covered List"), https://www.fcc.gov/supplychain/coveredlist, (Last visited June 26, 2026).

ensure that all Covered List sector devices are genuinely not produced in a foreign country or otherwise exempted. Under this targeted alternative proposal, we estimate the quantity of affected equipment to be below 10% of the overall equipment authorization applications submitted for the Commission's certification. We seek comment on this estimate. This more targeted approach would focus on the devices for -which component tracking is most critical to enforce the Commission's restrictions on authorizing covered equipment.

D. Software and other Components produced by Covered List entities

123. In the *Second Report and Order*, the Commission took its first step toward addressing component-level national-security risks in the equipment authorization program. The Commission prohibited the authorization of any device that incorporates a modular transmitter when that modular transmitter is itself covered equipment, even where the host device is not otherwise produced by an entity identified on the Covered List.[226] In the *Third Report and Order* above, the Commission has now extended the prohibition to devices containing logic-bearing hardware components produced by Covered List entities, while declining at this time to act on broader categories such as logic-bearing hardware, firmware, or software, and keeping the record open on those questions.[227] We build on that record here.

124. Now the Commission proposes to, and seeks comment on, prohibiting authorization for devices incorporating *any* components produced by a Covered List entity. Given that such entities have been found to produce or provide communications equipment or services that "pose unacceptable risks to the national security of the United States or the safety and security of United States persons," would such a rule advance national security or public safety objectives by prohibiting the authorization of dangerous devices? What would be the costs and benefits of such a rule? Would a rule covering *all* components be simpler and easier to comply with than our existing rules that cover devices containing certain specified components? Does the Commission have the legal authority to adopt such a rule that would include non-RF components like screws or nails that would otherwise be presumed not to directly cause interference? We note that the Secure Networks Act allows for the addition of devices to the Covered List for reasons independent of their ability to affect RF transmission or cause interference.[228] Moreover, recent National Security Determinations leading to additions to the FCC's Covered List have included concerns about supply chain dependencies, rather than direct compromise of communications.[229] Do devices that have a supply chain dependency on Covered List entities for components pose national security risks?[230] Does the Communications Act, the Secure Networks Act, and the Secure Equipment Act, or any other statute, individually or collectively give the Commission this authority?[231]

125. Alternatively, should the Commission adopt a rebuttable presumption against authorizing devices incorporating components produced by a Covered List entity, rather than categorically prohibiting

---

[226] *See, supra*, at para. 3.

[227] *See, supra*, at para. 13.

[228] For a piece of equipment to be added to the Covered List, the equipment must be "capable of—(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) *otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons*." 47 USC § 1601(b)(2).

[229] *See* Federal Communications Commission*, National Security Determination on the Threat Posted by Routers Produced by Foreign Countries*, March 20, 2026, https://www.fcc.gov/sites/default/files/NSD-Routers0326.pdf; Federal Communications Commission, *National Security Determination on the Threat Posed by Certain Uncrewed Aircraft Systems and Certain Uncrewed Aircraft Systems Critical Components*, January 7, 2026, https://www.fcc.gov/sites/default/files/NSD-FCC-Covered-List-Waiver0126.pdf.

[230] The President's National Security Strategy notes that "the United States must never be dependent on any outside power for core components." National Security Strategy at 13.

[231] *See, e.g.*, 47 USC §§ 151, 154(i), 302a, 1601-09.

the authorization of such devices? Under such an approach, the Commission would prohibit the authorization of devices incorporating any component produced by a Covered List entity unless the applicant for equipment authorization could demonstrate that the device incorporating such a component *does not* pose "unacceptable risks to the national security of the United States or the safety and security of United States persons," for example because the component cannot affect the RF emissions of the device or other reasons? If the Commission adopts such a rule, what standard should the Commission use for overcoming this presumption? Should we use a clear-and-convincing evidence standard, as we have in other proceedings, or should we use a less stringent preponderance of the evidence standard?[232] What would be the costs and benefits of this approach compared with a categorical prohibition discussed above?

126. In addition to hardware components, we also seek comment on how software and/or firmware produced or provided by a Covered List entity, if incorporated into another device, raises unacceptable national security risks. We note that following a specific determination from the Department of Commerce acting pursuant to Executive Order 13873, we have added to the Covered List, and therefore prohibited from equipment authorization, "equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software."[233] We also note that equipment on the Covered List is often controlled by software that is integrated onto the device.[234] For example, UAS, UAS critical components, and routers are often configured entirely through apps and receive software updates through remote device management platforms.[235]

127. We also note existing rules require software security features for authorized equipment. For example, all Bluetooth, WiFi, and other wireless devices operating in the unlicensed spectrum bands must "contain security features to protect against modification of software by unauthorized parties."[236] Our rules also require manufacturers "to take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio."[237]

128. Based on these potential risks, should the Commission prohibit the authorization of any device that has been integrated with the software or firmware that was produced or provided by a Covered List entity? Would such a prohibition address the potential "unacceptable risks" that such software or firmware could pose when integrated into an electronic device? What are the costs and benefits of such an approach? What alternative software, firmware and components are available once those produced by the named and identified entities on the Covered List are prohibited from getting authorized by the Commission? Alternatively, should the Commission adopt a rebuttable presumption against authorizing devices that have been integrated with the software or firmware that was produced or provided by a Covered List entity that can be overcome if an applicant demonstrates that such device does not pose

[232] *See, e.g.*, 47 CFR § 1.80003(e).

[233] FCC Covered List; Kaspersky Public Notice; Commerce Final Determination ("The Department finds that Kaspersky's provision of cybersecurity and anti-virus software to U.S. persons, *including through third-party entities that integrate Kaspersky cybersecurity or anti-virus software into commercial hardware or software*, poses undue and unacceptable risks to U.S. national security and to the security and safety of U.S. persons") (emphasis added).

[234] *DJI Android Go 4 Application Security Analysis,* Synacktiv (July 23, 2020) ("We found that . . . two features of the software that call home and wait for a file that orders the user's phone to install a forced update or install a new software. This mechanism is very similar to command and control servers encountered with malwares. . . . [a component] embedded in recent versions of DJI Android GO 4 application collects personal data such as IMSI, IMEI, the serial number of the SIM card, etc. This data is not relevant or necessary for drone flights and go beyond DJI privacy policy.").

[235] *See, e.g.,* Michael Fagan et al., Profile of the IoT Core Baseline for Consumer IoT Products, NIST IR 8425 (Sept. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf.

[236] 47 CFR § 15.407(i).

[237] 47 CFR § 2.944(a).

"unacceptable risks to the national security of the United States or the safety and security of United States persons?" The Commission seeks comment on the potential switching costs associated with transitioning to software, firmware, and components not produced by Covered List entities if such equipment produced by Covered list entities is prohibited, including any increased costs that may fall on U.S. producers, importers, retailers, or consumers. The Commission tentatively concludes that the annual costs of this proposal to be under $50 million and seek comment on our tentative assessment.

E. Requiring certification for devices in Covered List sectors

129. The Commission's rules require that no communications equipment produced by entities identified on the Covered List can obtain equipment authorization unless the authorization is obtained pursuant to the certification process, which is the most rigorous approval process for radio frequency devices.[238] This certification requirement applies even if the device would be otherwise subject to SDoC or an exemption from equipment authorization.[239] The Commission adopted these rules for equipment produced by a Covered List entity, because "the certification process provides the Commission with the necessary oversight to" fulfill its statutory mandate to prevent the authorization of covered equipment.[240] Under the certification process, applicants are required to make certain attestations (in the form of certifications) about the equipment for which they seek authorization, including attesting that the equipment is not covered and indicating whether the applicant is an entity identified on the Covered List.[241] Applicants are also required to submit supporting documentation and test data, which TCBs use to evaluate the devices, determine whether the devices meet all of the Commission's applicable technical and non-technical requirements, and ensure that the devices are not covered equipment.[242]

130. The Commission tentatively concludes that, just as devices produced by Covered List entities require the highest tier of Commission scrutiny and oversight, devices in Covered List sectors, such as UAS, UAS critical components, and routers, do as well. We seek comment on whether this framework should apply to Covered List sectors pursuant to a determination. We propose to amend 47 CFR § 2.907(c) to require any device from a Covered List sector to undergo the certification process even if otherwise eligible for authorization pursuant to a SDoC or exempt from equipment authorization. In other words, we propose to require UAS, UAS critical components, and routers—regardless of the producer or other characteristics of the device—to be subject to certification. We seek comment on this proposal, including the costs and benefits associated with this proposal. Should the Commission apply this proposal to any future Covered List sector?

131. We note that certification may also be vital for devices in Covered List sectors as a way to ensure that covered equipment cannot circumvent Covered List restrictions. The Commission's rules permit specific types of modules ("modular transmitters") to be authorized as "standalone" equipment, provided the equipment meets all applicable requirements. The rules provide that when an authorized modular transmitter is incorporated as a component part into another product, host, or device, no further equipment authorization is required insofar as the final product, host, or device conforms to the terms of the module's authorization. Noting that these modular transmitter rules created a potential loophole

---

[238] *See* 47 CFR 2.907(c) ("Any equipment . . . produced by any entity identified on the Covered List . . . must obtain equipment authorization through the certification process."); Federal Communications Commission, Equipment Authorization Procedures, https://www.fcc.gov/general/equipment-authorization-procedures. Last visited (June 30, 2026).

[239] *See*, Federal Communications Commission, Equipment Authorization Procedures, https://www.fcc.gov/general/equipment-authorization-procedures. Last visited (June 30, 2026).

[240] *EA Security R&O and FNPRM* at para. 78; *accord. id.* at para. 100.

[241] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13517-19, paras. 54-56; 47 CFR § 2.911(d)(5); *see also* § 2.932(e); § 2.1033(b); § 2.1043(b)(2)(i), (3)(i).

[242] *See, e.g.*, *EA Security R&O and FNPRM*, 37 FCC Rcd at 13514-16, 13518, paras. 48, 50, 52, 55; *see also, e.g.*, 47 CFR § 2.962(e).

regarding covered equipment, in the *Second Report and Order*, the Commission adopted rules to prohibit the authorization of equipment containing modular transmitters if the modular transmitters were themselves covered equipment.[243] Now that the Covered List contains production location-based covered equipment, the Commission seeks comment on whether there is a new loophole in our Covered List rules that could enable devices to circumvent the Commission's Covered List restrictions. As a result of our modular transmitter rules, devices in certain Covered List sectors (e.g., routers) that incorporate previously-authorized non-"covered" modular transmitters may be able to avoid the equipment authorization process altogether by relying on the FCC IDs that have been granted to the modular transmitters.

132. We seek comment on potential solutions to close this loophole. Would requiring certification for any device in a Covered List sector adequately reduce concerns that covered equipment in these sectors could skirt Commission restrictions using our modular transmitter rules? Are there other ways the Commission could close this loophole? Covered equipment is already prohibited from using the SDoC process under the rules adopted in the *First Report and Order*.[244] As national security vulnerabilities evolve, additional equipment may be identified and added to the Covered List, and any such newly added equipment would become subject to the same prohibitions. We seek comment on the expected volume of products that may be subject to the certification requirements each year. For example, would the number be on the order of 10,000 products annually, 100,000 products, or some other magnitude? We invite commenters to provide data, statistics, and other evidence to support their estimates.

133. Under the certification process, applicants must provide, (1), among other submissions, a written and signed certification that the equipment is not covered equipment; and (2) an affirmative or negative statement as to whether the applicant is identified on the Covered List as an entity producing covered communications equipment.[245] Should we amend 47 CFR § 2.911 to require additional disclosures as part of this certification process? If so, what, if any, additional information should applicants provide? In addition to HBOM and SBOM requirements that we sought comment on above,[246] should we, for example, require applicants to provide additional contact information for the producer(s) of the device and/or components to allow for TCB or Commission verification of the production location information? The Commission tentatively concludes that the additional contact information required under this proposal would impose, at most, the equivalent of one hour of an office administrator's time per application. We seek comment on this preliminary assessment, including whether this estimate accurately reflects the expected burden.

F. Importation under 2.1204

134. Section 2.1204 of the Commission's rules sets forth conditions that must be met before radio frequency devices may be imported into the United States. As presently drafted, however, these conditions do not distinguish between covered equipment and non-covered equipment. As such, parties could conceivably use the ability to import covered equipment in limited quantities by operation of one of several pre-authorization import conditions. We tentatively conclude that we should close this loophole by excluding covered equipment from section 2.1204(a) entirely and by creating a new subsection in section 2.1204 to provide a narrow set of conditions for importing Covered List equipment. We seek comment on this proposal, both generally, and in the following specific areas.

1. Conditions for Importation of Covered List Equipment

135. Because covered equipment cannot receive new authorizations from the FCC, we propose

[243] *Second Report and Order,* at para. 3.

[244] *First Report and Order*, 37 FCC Rcd 13496, para. 3.

[245] *See* 47 CFR § 2.911(d)(5).

[246] *See*, infra, para. 118.

to modify section 2.1204(a) of our rules ("Import conditions") to expressly exclude covered equipment and to add a new paragraph to govern the conditions under which covered equipment may be imported without an equipment authorization. Specifically, we propose to permit the importation of covered equipment only when such equipment meets one or more of the following conditions: (a) has a valid equipment authorization that has not been limited through the process set forth in section 2.939(e); (b) is being imported in a quantity of 40 or fewer units for testing and evaluation or product development, unless the Chief of OET grants written approval for a greater quantity; (c) is being imported solely for export; (d) is being imported for the exclusive use of the U.S. Government; or (e) is being imported solely for the purpose of developing products to be marketed exclusively to the U.S. Government or pursuant to federal contracts. We seek comment on this proposal. Are there additional conditions under which we should allow covered equipment to be imported?

2. Testing and Evaluation Unit Quantity

136. The Commission's current regulations allow importation of 4,000 or fewer unauthorized radiofrequency devices from a given model if the devices are being imported for testing and evaluation to determine compliance with FCC rules and regulations, product development or suitability for marketing.[247] The Commission also permits a greater number of devices to be imported if the OET Chief provides written approval.[248] We tentatively conclude that 4,000 units is an unreasonably large number of unauthorized covered equipment devices to be imported, and that importation to determine suitability for marketing covered equipment is never reasonable, given that the marketing and sale of such equipment is prohibited. We tentatively conclude, based on our experience dealing with device testing, that 40 devices for a given model seems to be sufficient for testing and evaluation and evaluation and product development. Are 40 units sufficient for testing and evaluation? Would a smaller number be sufficient? Is a greater number needed? If larger or smaller numbers are needed for these purposes, commenters should explain why. Additionally, should the Commission continue to allow the Chief of OET to provide written approval for the importation of a greater number of a certain model of covered equipment, as is currently allowed in the Commission's importation rules?[249] Should there be any limits on the OET Chief's discretion?

3. Import for Export

137. Section 2.1204(a)(5) of the Commission's rules, the "import for export" condition, allows unauthorized devices to enter the United States so long as the equipment is being imported solely for export and is not marketed within the United States.[250] The Commission proposes to maintain this condition as an option to import unauthorized covered equipment in a new section (b), because importation of the device solely for re-export does not pose the same risks as importing the device of use or sale in the U.S. market. We seek comment on this proposal.

138. Separately, and independent of the Covered List, subsections 2.1204(a)(5)(i)-(ii) create exceptions that allow the marketing of unauthorized cellphone handsets and similar devices that are only capable of functioning outside of the United States.[251] The rationale given for these exceptions in 1999

[247] 47 CFR § 2.1204(a)(3).

[248] 47 CFR § 2.1204(a)(3)(i).

[249] 47 CFR § 2.1204(a)(3)(ii).

[250] 47 CFR § 2.1204(a)(5).

[251] The Commission's rules prohibit the marketing of import for export equipment unless: 1) the device is a foreign standard cellular phone solely capable of functioning outside the U.S., or 2) the device is a multi-mode wireless handset that has been certified under the Commission's rules and a component (or components) of the handset is a foreign standard cellular phone solely capable of functioning outside the United States. 47 CFR § 2.1204(a)(5)(i)-(ii).

was that the phones operate on standards not used in the United States and thus cannot function here.[252] We tentatively conclude that the exceptions in paragraphs (a)(5)(i)-(ii) should be eliminated, thereby removing the exception permitting the marketing of unauthorized cellphone handsets and similar devices that are only capable of functioning outside of the United States. There seems to be no need to market devices in the U.S. that cannot operate in the U.S. Accordingly, we seek comment on whether this exception should be maintained. Are there currently domestic entities that benefit from the import for export trade in these cellphones? If operated within the United States, could these exempted foreign cellphones increase the potential for interference to communications or introduce an unacceptable national security risk through, for example, a Wi-Fi firmware update? We seek comment regarding methods that would assist in positively identifying cellphone equipment that is only capable of functioning outside of the United States.

4. Government Use Exclusion

139. Section 2.1204(a)(6) reflects a statutory provision that permits the importation of unauthorized (or not-yet-authorized) equipment exclusively for U.S. Government use.[253] We therefore propose to preserve this condition for the importation of unauthorized covered equipment. We also propose to expand this condition for unauthorized covered equipment to also include equipment that is imported for the purpose of developing other products that are exclusively for federal use. Would such exemptions be in the public interest? For example, might defense contractors want to import the latest models of foreign-produced UAS to develop their products? If so, what type of documentation would be necessary and sufficient to permit CBP to verify the import condition at the port of entry or prior to its arrival? What additional safeguards or procedures should we place on the importation of Covered List equipment for this purpose?

5. Importation for Personal Use

140. The Commission's import rules also permit a limited exception for an individual's personal use.[254] Section 2.1204(a)(7) permits the importation of up to three devices, in specified categories, that are not intended for sale.[255] Given that compromised Covered List devices could be networked to present a greater threat vector, we seek input on whether any specific types of covered equipment should be excluded from the exemption or whether the personal use exemption should be wholly eliminated for Covered List equipment. Further, we propose, for purposes of section 2.1204(a)(7),

---

[252] "These types of devices may continue to be imported and marketed for use outside of the U.S." Federal Communications Commission, Importation of Devices Capable of Causing Harmful Interference, 64 Fed. Reg. No. 248 72571. (Dec. 28, 1999).

[253] *See* 47 U.S.C. § 302a(c); 47 CFR § 2.1204(a)(6).

[254] Webster's defines "personal" as, *inter alia*, "intended for private use or use by one person." *See* https://www.merriam-webster.com/dictionary/personal. We note that the term personal use is also used, without definition, in the context of homemade radiofrequency devices. "Equipment authorization is not required for devices that are not marketed, are not constructed from a kit, and are built in quantities of five or less for personal use." 47 CFR § 15.23(a) (requiring the use of good engineering practices to prevent interference).

[255] Three unauthorized devices for personal use may only be from one the following categories:

> (i) Unintentional radiator as defined in part 15 of this chapter which may include radio receivers, computers or other Class B digital devices in part 15 of this chapter.
>
> (ii) Consumer ISM equipment as defined in part 18 of this chapter.
>
> (iii) Intentional radiators subject to part 15 rules only if they can be used in client modes as specified in § 15.202 of this chapter.
>
> (iv) Transmitters operating under rules which require a station license as subscribers permitted under § 1.903 of this chapter and operated under the authority of an operator license issued by the Commission.

47 CFR § 2.1204(a)(7).

to define "personal use" as applying to a device which will be used: (1) in a manner not intended for sale, lease, marketing, distribution, or other commercial advantage; and (2) solely by an individual or a not-for-profit entity for noncommercial purposes. We seek comment on the appropriate meaning of the term "personal use" in this context. Should "personal use" be defined in the same manner for purposes of section 15.23 of the Commission's rules?[256]

6. Other importation exceptions

141. We seek comment on whether any other exclusions to the ban on unauthorized radio frequency device importation should be modified. For instance, should the section 2.1204(a)(4) exclusion permitting limited numbers of devices for demonstration at trade shows be revised in any way? Should the section 2.1204(a)(8) exclusion permitting importation for repair of an item be retained or revised in any way? Should the section 2.1204(a)(9) exclusion allowing importation of medical implant transmitter inserted in a person or a medical body-worn transmitter be retained or amended in any way? Should the 2.1204(a)(10) exclusion permitting portable earth-station transceivers be retained or amended? Should the 2.1204(a)(11) exclusion allowing imported in quantities of 12,000 or fewer units for pre-sale activity be retained or amended in any way? Should the Commission adopt any other exclusion?

142. These proposed exclusions would relax the importation prohibition rules only under narrowly defined and highly targeted conditions. Given the limited scope of these circumstances, the Commission expects that this proposal would yield net economic benefits by reducing compliance costs without introducing additional national security risks. We seek comment on this assessment.

G. Marketing under 2.803

143. "Marketing" is defined to include "sale or lease, or offering for sale or lease, including advertising for sale or lease, or importation, shipment, or distribution for the purpose of selling or leasing or offering for sale or lease."[257] In this *Third Further Notice*, we seek additional comment on any methods that will further restrict the marketing and operation of Covered List equipment within the United States.

1. Limiting Marketing of Radiofrequency Devices Without an Authorization

144. Presently, section 2.803(c) of our rules permits limited marketing of a radiofrequency device before the device has been authorized.[258] While this flexibility promotes innovation by increasing the speed with which a company can bring a new device to market, the rule, as currently framed, has the potential to create marketplace confusion or subversion of our other rules by suggesting that entities might still engage in marketing of devices on the Covered List under the guise of permitted "pre-authorization" marketing activities, even though such devices cannot receive equipment authorizations under our rules. We therefore tentatively conclude that the authority to engage in marketing of radio frequency devices without an authorization should expressly exclude radiofrequency devices that are covered equipment and propose to establish a separate general rule under section 2.803 that prohibits the marketing of covered equipment that was authorized prior to inclusion on the Covered List. To that end, we seek comment on the extent to which unauthorized Covered List equipment is currently being marketed in the United States under section 2.803(c). Are there circumstances where marketing of unauthorized Covered List equipment should be permitted (for example, to the United States government)? If so, what conditions should we place on such marketing?

145. To ensure uniformity in the application of section 2.803, we also tentatively conclude that two additional changes to this section are prudent. First, we propose to change the title of the rule to "Marketing of radiofrequency devices that lack an equipment authorization." Section 2.803(b) expressly permits the marketing of equipment that has been authorized pursuant to a valid FCC equipment

[256] 47 CFR § 15.23.

[257] 47 CFR § 2.803(b).

[258] *Id.* § 2.803(c).

authorization, and a recent amendment to this rule prohibits the marketing that has been limited through the procedures described in section 2.939(e).[259] Second, we propose an express exclusion of Covered List devices from exceptions set forth in section 2.803(c). In other words, we propose to amend our rules to exclude unauthorized covered equipment from the exceptions in section 2.803(c). We seek comment on these additional modifications of section 2.803 as a means of closing pathways for marketing unauthorized Covered List equipment.

146. These proposed rules may introduce minor delays in stakeholders' marketing plans; however, such delays could prevent wasted marketing efforts in situations where equipment is later determined to be covered equipment and consequently prohibited. By reducing the likelihood of unsuccessful or non-compliant marketing activities, the rule offers clarity that can ultimately conserve stakeholder resources. Moreover, we see substantial national security and public safety benefits from this rule by limiting opportunities for the marketing of new models of covered equipment, which have been determined to pose "unacceptable risks to the national security of the United States or the safety and security of United States persons."[260] Accordingly, the Commission tentatively concludes that the benefits of eliminating ambiguity through this clarification are likely to outweigh the modest costs associated with potential marketing delays. We seek comment on this assessment.

2. Disclosure of Device Brand Names and Model Names

147. Entities identified on the Covered List may attempt to enter the U.S. market through the practice of creating new, seemingly unaffiliated brand names. A rash of new brand names that are still affiliated with Covered List entities could stymie inspections at ports of entry and could evade detection by online marketplaces. Similarly, unaffiliated white label online marketplaces could continue, or begin, to market the equipment under their own brand name. We seek comment on the best means to identify the marketing of authorized, limited, and revoked Covered List equipment that is being marketed within the United States. Should all applicants for equipment authorization and grantees be required to disclose the brand names under which they operate? Should grantees be required to disclose, in confidential submissions, the brand names of authorized equipment produced for other entities under white labeling arrangements? Should the Commission require that grantees keep updated a list of brand names under which devices are sold? Should applicants and grantees be required to disclose all model names corresponding to each FCC ID? We tentatively estimate that such disclosures require no more than one hour of an office administrator's time and seek comment on this estimate. Alternatively, should disclosure of brands and white-labeled devices be required only of Covered List entities and their subsidiaries and associates? Is there any analogous process that could be implemented to address SDoC devices, which are not recorded in OET's EAS database?

3. Prohibiting Marketing and Using for Illegal or Unlawful Purposes

148. As Americans rely on an increasing number of wireless and connected devices, there is an increased opportunity to use otherwise lawful radio frequency devices for illegal or unlawful purposes. For example, a certified software defined radio (SDR) platform designed for research can, with the right know-how, be modified, either physically or through software, to operate in an illegal manner (i.e., at variance from its certified parameters) or for an unlawful purpose. With the increased prevalence of SDRs and the development of similar software-based technologies, we are concerned that otherwise lawful devices might be marketed in a manner that highlights the potential unlawful operation capability or in a way that promotes the ability of an end user to modify a lawful device to operate illegally. Accordingly, we propose to adopt rules that would restrict individuals and entities from engaging in marketing activities that promote the ability to use a radio frequency device subject to an FCC authorization (either a certification or an SDoC) for illegal purposes or the ability of the end user to

[259] Pursuant to section 2.939(e), the Commission will consider both public comment and the public interest to determine whether the importation and marketing of covered devices that have an existing authorization should continue or be prohibited. 47 CFR § 2.939(e).

[260] 47 USC § 1601(c).

modify the device to operate at variance from its authorized parameters. We seek comment on this proposal. Do we have authority to impose such a restriction on marketers of radio frequency equipment? If not, should we prescribe information that must be included in any marketing materials to prevent the promotion of marketing for illegal or unlawful uses of lawful devices or that caution end users against modifying devices to operate outside of their authorized parameters? What standard should we use to determine whether a marketer is promoting an illegal or unlawful activity? What standard should we use to assess whether a marketer is promoting how a device can be modified or the ease with which it can be modified? To the extent that a marketer of radio frequency devices promotes illegal or unlawful uses or illegal or unlawful modifications of an authorized device, should our enforcement mechanisms account for revenues or profits generated from such activity? Would our proposal, or any alternative proposals, be consistent with any applicable First Amendment requirements?

149. In addition to authorized devices, there are radio frequency devices (e.g., transmitters capable of operating solely on frequencies allocated to the Amateur Radio Service) that do not require equipment certification because they are intended for use only by licensed operators within their authorized service.[261] However, some retailers market equipment that is capable of operating outside these exempt frequency bands—such equipment requires certification, and its marketing and operation violate our rules if the proper certification is not obtained.[262] We propose that marketers, including online marketplaces, of such devices must prominently display the following warning at the point of sale, including any online advertisement, to advise unwary consumers: "This equipment may only be sold to end users in the United States who hold the appropriate FCC license. Information regarding the purchase will be provided in response to a request by the FCC." Do we have authority to adopt this proposal, consistent with the Communications Act and the First Amendment? Consumers who operate such equipment without the appropriate license are already subject to enforcement action. Unlicensed consumers who purchase such equipment, despite the consumer warning, and operate it at variance with our rules would then be subjected to an enhanced penalty. We seek comment, particularly from manufacturers, distributors, and retailers, regarding how such rules would affect the marketplace for this equipment. We also seek comment on whether sales to unlicensed end users should be strictly prohibited. Certain licensee information is publicly available in Commission databases. Is it feasible to require retailers to obtain proof of licensure and verify that information prior to the sale?

150. We estimate that the verification required under this proposal may take no more than one hour for retailers to confirm each buyer's license prior to sale. We seek comment on this estimate, including whether stakeholders anticipate greater or lesser burdens in practice. We also seek comment on the expected volume of products that may be subject to the verification requirements each year. For example, would the number be on the order of 10,000 products annually, 100,000 products, or some other magnitude? We invite commenters to provide data, statistics, and other evidence to support their estimates. While such verification might be easily accomplished in a brick-and-mortar retail establishment, would such a verification be unduly burdensome for online marketplaces? If so, what alternatives might we enact to ensure that type-excepted equipment is only sold to authorized end users?

151. Given the potential for dual use of radio frequency equipment authorized pursuant to a certification or SDoC, we propose to modify parts 2 and 15 of our rules to establish that FCC-authorized

[261] See 47 C.F.R. § 97.301(a) (amateur allocations).

[262] *ABC Fulfillment Services LLC d/b/a HobbyKing USA LLC and HobbyKing.com,* Citation and Order, 32 FCC Rcd 7300, para. 4 n.5 ("Although HobbyKing identifies the AV transmitters as operating on amateur frequencies, the equipment is also apparently able to operate outside of the amateur frequencies and, in some cases, at higher power levels than allowed, making the equipment non-compliant under the Act and Commission's rules."); *New Generation Hobbies*, Citation, 26 FCC Rcd 9468, 9471 n.23 (EB SED 2011) ("while amateur radio service equipment is exempt from the FCC's equipment certification requirement, it is a violation of the Commission's regulations to market in the United States a transmitter that is designed or intended to operate on frequencies outside of the authorized amateur radio service bands if such equipment has not been issued a grant of equipment certification").

radio frequency equipment, including type-accepted equipment, cannot be used to facilitate criminal acts. Currently, Amateur Radio Service licensees are prohibited from transmitting "communications intended to facilitate a criminal act."[263] Likewise, General Mobile Radio Service licensees may not use their stations to communicate "[m]essages in connection with any activity which is against Federal, State, or local law."[264] Should we impose a similar restriction for all FCC-authorized radio frequency devices? If such a restriction would not be beneficial for all devices, should we instead impose this restriction only on unlicensed devices authorized pursuant to part 15 of our rules? Should there be any exceptions to such a rule? We also note Section 705 of the Communications Act already prohibits the unauthorized publication or use of communications, including unauthorized interception of radio communications.[265] How can this prohibition be enforced to mitigate against the risks identified in specific national security determinations?

H. Use of FCC Logo, 47 CFR § 2.1074

152. Until 2017, the FCC logo was required on equipment that was authorized by the former Declaration of Conformity equipment authorization procedure. During a 2017 rulemaking proceeding, the Commission merged the Declaration of Conformity procedures into the new SDoC authorization and reconsidered whether this labeling requirement was still needed.[266] Acknowledging that the FCC logo is "a symbol of compliance" and "its presence can assist customs officers, entities in foreign countries, and others who may want to know whether a device complies with our rules,"[267] the Commission codified a rule that makes the use of the FCC logo voluntary for SDoC devices.[268] Although this rule makes clear that the FCC logo is intended signify that the device complies with the applicable rules, the Commission did not create a parallel rule for certified devices nor did it establish a regulatory structure that prevents use of the logo on an unauthorized device.[269]

153. We seek comment on whether voluntary use of the FCC logo aids enforcement of our equipment authorization rules and whether its use should be continued. If so, should we establish a rule that extends the current practice to certified devices? The Commission has encountered a significant number of inquiries from our federal partners at CBP regarding equipment that appears to be unauthorized while displaying the FCCs logo.

154. Additionally, in some instances, the Commission has observed that equipment manufacturers have placed the FCC logo on devices that incidentally generate radio frequency energy, known as an "incidental radiator,"[270] which do not generally require an FCC equipment authorization.[271]

---

[263] 47 CFR § 97.113(a)(4).

[264] 47 CFR § 95.1733(a)(1).

[265] 47 USC § 605.

[266] *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, First Report and Order, FCC 17-93 para. 18 (2017).

[267] *Id.* (citing TCB Council Comments at 2).

[268] 47 CFR § 2.1074(b) ("Devices subject to authorization under Supplier's Declaration of Conformity may be labeled with the following logo on a voluntary basis as a visual indication that the product complies with the applicable FCC requirements.).

[269] *See* Office of Engineering and Technology, Federal Communications Commission, *KDB 784748, Product Labelling/Manuals & Packing FCC Disclosures*. Nov. 2, 2023, https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?switch=P&id=27980.

[270] 47 CFR § 15.3(n) (defining an incidental radiator as "[a] device that generates radio frequency energy during the course of its operation although the device is not intentionally designed to generate or emit radio frequency energy. Examples of incidental radiators are dc motors, mechanical light switches, etc.").

[271] Incidental radiators need only be manufactured to minimize the risk of harmful interference. *See* 47 CFR § 15.13.

We propose that use of the FCC logo should be prohibited from use on incidental radiators because such devices do not require authorization. Using the FCC logo on incidental radiators may be misleading for consumers, who might incorrectly assume that the device has somehow been given the FCC's "stamp of approval." Restricting stakeholders from using the FCC logo on devices outside the authorization framework, the Commission tentatively concludes that this proposed rule would not impose incremental costs on regulated parties. We seek comment on this tentative conclusion and general benefits and costs associated with this proposal.

155. Likewise, the Commission has observed the marketing of unauthorized radio frequency devices with the FCC logo. Our rules prohibit deceptive use of certification,[272] and SDoC procedures,[273] but there is no rule that specifically prohibits the misuse of the FCC logo.[274] We propose to expressly prohibit the use of the FCC logo on any device that has not been properly tested and authorized under our rules and seek comment on this proposal. We also seek comment on other proposals to protect consumers and the public from misleading uses of the FCC logo, such as through civil action for a false designation of origin claim under the Lanham Act.[275]

156. Finally, we seek comment on whether the Commission should adopt other rules regarding the FCC logo. For example, should the Commission *require* the use of the FCC logo for all RF devices that have been validly authorized—pursuant to FCC certification or SDoC? What would the costs and benefits of such a proposal be?

I. Streamlined revocation, 47 CFR § 2.939

157. We propose to adopt a streamlined procedure for revoking equipment authorizations. Under our current rules, revocation of an equipment authorization must proceed "in the same manner as revocation of radio station licenses," except in cases subject to the expedited processes applicable to covered communications equipment in cases in which there has been a false statement or representation in the certification application or associated materials.[276] This radio station license framework dates back more than 70 years, when the Commission first unified its equipment authorization rules, which had previously been dispersed across various radio service rule parts.[277] At that time, the Commission noted that authorization holders relied on approval but emphasized that it assumed "no responsibility in granting type acceptance [equipment authorization] that the equipment will always comply," and it relied on the general appeal procedures in the rules to allow parties to seek Commission review of denials or withdrawals.[278]

158. The equipment authorization landscape, particularly following the creation of the Covered List and the passage of the Secure Equipment Act requiring the Commission to prohibit certain

[272] 47 CFR § 2.927(c) (prohibiting deceptive use of a certification).

[273] 47 CFR § 2.1072 (prohibiting deceptive use of SDoC).

[274] *See* Office of Engineering and Technology, Federal Communications Commission, *KDB 784748, Product Labelling/Manuals & Packing FCC Disclosures*. Nov. 2, 2023, https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?switch=P&id=27980.

[275] 15 USC § 1125(a).

[276] 47 CFR § 2.939 (d).

[277] FCC 55-61, Federal Communications Commission, No. 20, Fed. Reg. 337-343; noting that prior rules for withdrawal of type approval did not specify a process for revocation, see, e.g., 47 CFR 18.16 in Federal Communications Commission, No. 15, Fed. Reg. 533. ("A certificate of type approval may be withdrawn if the type of approval equipment for which it was issued proves defective in service and under usual conditions of maintenance and operation such equipment cannot be relied on to meet the conditions set forth. in this part for the operation of the type of equipment involved").

[278] *Id*. The Commission would later redesignate this rule as one pertaining to equipment authorization, *see* FCC 74-113, 45 F.C.C.2d 52.

authorizations on national security grounds, has changed substantially since those early rules were adopted. As a result, the legacy procedures governing revocation of equipment authorizations are no longer aligned with our approach to similar vulnerabilities and create a gap in the Commission's overall risk-mitigation framework.

159. We seek comment, for example, on whether we should remove section 2.939(b) entirely, or revise section 2.939(d) of our rules to adopt the streamlined proceeding adopted in the *First Report and Order* for any revocation involving willfulness, such as false statements or misrepresentations to the Commission, test labs, or TCBs involving an equipment authorization application or existing grant.[279] We also seek comment on whether this streamlined revocation procedure should also include any false statements or misrepresentations submitted to the Commission and/or DoW and DHS as part of an application for, or maintenance of, a "Conditional Approval" to have a device removed from the Covered List or any similar process to have certain devices removed from the Covered List.[280] For example, to apply for Conditional Approval, applicants must submit a substantial amount of information, including information concerning corporate structure and an onshoring plan.[281] Notably, grants of Conditional Approval will be terminated if applicants "knowingly violate the terms of the Conditional Approval or materially misrepresent information provided the U.S. Government."[282] We propose to direct OET to automatically initiate a streamlined revocation process for any equipment authorizations granted pursuant to a Conditional Approval that is terminated on one or more of these grounds.

160. Should we also include willful failure to provide the Commission or a TCB (or DoW and/or DHS if related to a Conditional Approval) with updated information, such as the willful failure to provide updated information on a changed agent for service of process in the United States, as required by the Commission's rules?[283] We also seek comment on applying this procedure to all revocations involving covered equipment. Given that such equipment has been found to "pose unacceptable risks to the national security of the United States or the safety and security of United States persons,"[284] the Commission tentatively concludes that "public health, interest or safety"[285] might require rapidly revoking authorizations to import, market, and operate this equipment. The Commission further tentatively concludes that the public interest associated with swift revocation is likely to outweigh the costs borne by entities affected by a streamlined revocation decision. We seek comment on this tentative

[279] *See* 5 USC § 558(c) (allowing for streamlined revocation in cases of "willfulness").

[280] UAS, UAS critical components, and routers—even if produced in a foreign country—are not on the Covered List if they "have been granted a Conditional Approval by DoW or DHS." *See* FCC Covered List.

[281] *See* Federal Communications Commission, *Guidance on Submissions for Conditional Approval for Uncrewed Aircraft Systems (UAS) and UAS Critical Componetns Produced in Foreign Countries Subject to the FCC's Covered List*, Jan. 7, 2026, https://www.fcc.gov/sites/default/files/UAS-Guidance-Submissions-Conditional-Approvals.pdf; Federal Communications Commission, *Annex A: Guidance on Submissions for Conditional Approval for Routers Produced by Foreign Countries Subject to the FCC's Covered List*, Mar. 20, 2026, https://www.fcc.gov/sites/default/files/Guidance-for-Conditional-Approvals-Submissions0326.pdf.

[282] *See* Federal Communications Commission at 1, *Guidance on Submissions for Conditional Approval for Uncrewed Aircraft Systems (UAS) and UAS Critical Componetns Produced in Foreign Countries Subject to the FCC's Covered List*, Jan. 7, 2026, https://www.fcc.gov/sites/default/files/UAS-Guidance-Submissions-Conditional-Approvals.pdf; Federal Communications Commission at 1, *Annex A: Guidance on Submissions for Conditional Approval for Routers Produced by Foreign Countries Subject to the FCC's Covered List*, Mar. 20, 2026, https://www.fcc.gov/sites/default/files/Guidance-for-Conditional-Approvals-Submissions0326.pdf.

[283] 47 CFR § 2.929(c); *Eken Group Limited*, Notice of Liability for Forfeiture, FCC 24-122, 39 FCC Rcd 12990 (2024) (proposing $730,000 statutory maximum civil penalty against a foreign doorbell camera manufacturer for submitting false certifications under section 2.911(d) regarding its U.S. agent for service of process).

[284] 47 USC §§ 1601(b)(1), (c).

[285] *See* 5 USC § 558(c) (allowing for streamlined revocation in "those [cases] in which public health, interest, or safety requires").

conclusion, including whether commenters believe the balance of benefits and costs differs under any particular circumstances. We further seek comment on how the service of process should be effected under these revocation rules, particularly for foreign grantees that may attempt to evade the jurisdiction of U.S. law. Is service of process legally required if grantees of actual or constructive notice?

161. Additionally, we seek comment on changing our rules to allow for a streamlined revocation process that nonetheless comports with the three-step process for revocation required by the Administrative Procedure Act (APA), even where willfulness is not present. The APA only requires "[e]xcept in cases of willfulness or those in which public health, interest, or safety requires otherwise," that "before the institution of agency proceedings" to revoke, "the licensee has been given (1) notice by the agency in writing of the facts or conduct which may warrant the action; and (2) opportunity to demonstrate or achieve compliance with all lawful requirements."[286] The Commission's rules requiring the radio station license process therefore requires substantially more process than is statutorily required.[287] Should we instead adopt the streamlined revocation procedures that the Commission recently utilized in several international section 214 authorization procedures and recently codified in the submarine cable license context?[288] How might such proceedings facilitate the efficient functioning of government and rapid removal of dangerous equipment from the U.S. market? Would such proceedings undermine the due process rights of grantees?

J. Permitting permissive changes for basic software and hardware updates, even for "covered" equipment

162. We propose to codify in our rules a limitation on the prohibitions in sections 2.932(b) and 2.1043(b) for certain Class I and Class II permissive changes to covered equipment. In particular, we propose to incorporate into our rules a framework permitting software and firmware updates that mitigate harm to U.S. consumers for already-authorized covered equipment. We also seek comment on the exact scope of permissive changes to permit and what types of covered equipment should be eligible.

163. *Background*. On December 22, 2025, the FCC added to the Covered List uncrewed aircraft systems (UAS) and UAS critical components produced in foreign countries. On March 23, 2026, the FCC added to the Covered List "[r]outers produced in a foreign country, except routers which have been granted a Conditional Approval by DoW or DHS"[289] (Covered Routers).

164. On January 21, 2026, OET announced a waiver of certain prohibitions contained in 47 CFR §§ 2.932(b) and 2.1043(b) for UAS and UAS critical components produced in a foreign country, which were added to the Covered List on December 22, 2025. The waiver permitted all UAS and UAS critical components authorized for use in the United States to continue to receive software and firmware

[286] 5 USC § 558(c).

[287] *See* 47 CFR § 2.939(b) ("Revocation of an equipment authorization shall be made in the same manner as revocation of radio station licenses" except in limited circumstances); 47 U.S.C. § 312(c) (revoking a radio station license requires a hearing or a waiver).

[288] *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks,* OI Docket No. 24-523, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-49, 40 FCC Rcd 6481, 6508-16 paras. 50-58 (2025) (citing *China Telecom Americas Order on Revocation and Termination*, 36 FCC Rcd 1618 (2021); *China Unicom Americas Order on Revocation*, 37 FCC Rcd 1480 (2022); *Pacific Networks and ComNet Order on Revocation and Termination*, 37 FCC Rcd 4220 (2022)).

[289] *Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List,* WC Docket No. 18-89, Public Notice, DA 26-278 (Mar. 23, 2026) (*Routers Public Notice*). For the current version of the Covered List and Conditional Approvals, see Federal Communications Commission, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist.

updates that mitigate harm to U.S. consumers at least until January 1, 2027.[290] On March 23, 2026, OET announced a similar waiver of these prohibitions for covered routers added to the Covered List earlier that day.[291]

165. The waivers of Class I permissive changes were necessary to account for newly adopted revisions of rule sections 2.932(b) and 2.1043(b), which excluded equipment prohibited from authorization pursuant to § 2.903 from equipment certification procedures that otherwise typically allow for permissive changes to authorized equipment.[292] This effectively prevented previously authorized devices from receiving essential updates solely because they had become newly identified as "covered." The prohibited changes include Class I permissive changes, which generally do not require a filing with the Commission and may include software, firmware, and security updates to mitigate harm to U.S. consumers. The waivers permitted all UAS and UAS critical components and Routers authorized for use in the United States to continue to receive software and firmware updates that mitigate harm to U.S. consumers.

166. On May 8, 2026, OET announced an extension of these waivers until January 1, 2029, and an expansion to cover similar software and firmware permissive changes that are classified as Class II permissive changes, because they "degrade the performance characteristics as reported to the Commission at the time of the initial certification."[293] OET also noted that this extension would give it time to recommend the Commissioner consider a rulemaking on this matter,[294] which OET does here in this *Third Further Notice*.

167. We propose to codify, and make permanent, this waiver with respect to all already-authorized covered equipment. Specifically, we propose to amend sections 2.932(b) and 2.1043(b) to clarify that that such minor software and firmware updates that mitigate harm to consumers do not constitute applications for equipment authorization—which the Commission is forbidden from granting under the Secure Equipment Act—and are therefore permitted under Commission rules.[295] We envision that this exception to the general prohibition would include software or firmware updates necessary to maintain existing functionality, security or vulnerability patches, and updates required to maintain compatibility with supported operating systems or protocols. We seek comment on this approach. Should the FCC define the category of software and firmware permissive changes differently? What are the national security benefits from allowing continued software and firmware security updates? Are there any national security drawbacks to this approach? Is it consistent with Congress' statutory directive, as well as broader national security determinations? Should we only allow for these software and firmware updates for already-authorized covered equipment in a production location-based Covered List entry, rather than covered equipment in a producer/provider-based Covered List entry? In other words, should

[290] *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered UAS and UAS Critical Components,* ET Docket No. 21-232, Public Notice, DA 26-69 (Jan. 21, 2026).

[291] *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered Routers,* ET Docket No. 21-232, Public Notice, DA 26-286 (Mar. 23, 2026).

[292] 47 CFR §§ 2.932(b), 2.1043(b); *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered UAS and UAS Critical Components,* ET Docket No. 21-232, Public Notice, DA 26-69 (Jan. 21, 2026); *Office of Engineering and Technology Announces Waiver of Prohibitions on Certain Class I Permissive Changes to Covered Routers,* ET Docket No. 21-232, Public Notice, DA 26-286 (Mar. 23, 2026).

[293] 47 CFR 2.1043(b)(2); *Office of Engineering and Technology Announces Extension and Expansion of Waiver of Prohibitions on Certain Software and Firmware Permissive Changes to Certain Covered UAS, UAS Critical Components, and Routers*, ET Docket 21-232, Public Notic e, DA 26-454 (May 8, 2026).

[294] 47 CFR 2.1043(b)(2); *Office of Engineering and Technology Announces Extension and Expansion of Waiver of Prohibitions on Certain Software and Firmware Permissive Changes to Certain Covered UAS, UAS Critical Components, and Routers*, ET Docket 21-232, Public Notic e, DA 26-454 (May 8, 2026).

[295] *Second Report and Order*, para. 55; Secure Equipment Act § 2(a)(2).

we permit an already-authorized router produced abroad to be able to receive these updates, but not an already authorized covered telecommunications device?

168. Furthermore, the Commission seeks comment on whether we should extend this allowance to any type of Class I and/or Class II permissive changes involving certain minor hardware modifications to certain already-authorized covered equipment? Should the Commission allow minor component replacements? What are the costs and benefits of extending this allowance to hardware? If the Commission permits hardware permissive changes to already-authorized covered equipment in a production location category, the Commission proposes to limit these modifications to the following:

169. (a) The modification mitigates harm to consumers;

170. (b) The modification involves the replacement of one component for another component at the same location in the device;

171. (c) The modification does not enhance the device's capability or alter its intended use;

172. (d) The modified device is marketed as an identical product to the pre-modified device;

173. (e) The modified device is equipment in a producer/provider-based Covered List entry, rather than a production location-based Covered List entry; and

174. (f) The modification does not involve the replacement of a U.S.-produced component for a foreign-produced component.

175. We seek comment on each of these proposed limits. We believe this would allow for hardware permissive changes that do not undermine national security. Is this an appropriate limitation, or should the Commission adopt some sort of variation? What are the costs and benefits of this approach? Additionally, should we require that any Covered List entity that engages in the above listed modifications notify the FCC? Should we require such entity notifies its consumer base? Would such measures enhance security of said covered equipment?

176. The Commission tentatively concludes that allowing permissive updates and changes to software, firmware, and hardware would reduce consumer harms while not introducing additional national security risks. In this respect, we preliminarily find that the proposal is likely to produce a net increase in benefits for consumers and other stakeholders. We seek comment on this tentative conclusion, including whether commenters anticipate any circumstances in which such permissive updates could alter this cost-benefit assessment.

K. Operation of RF devices prior to equipment authorization

177. We propose to revise our rules concerning operation of RF devices prior to equipment authorization in section 2.805[296] to conform with our proposed changes to our equipment marketing and importation rules. Are the current safeguards against marketing or importation of devices prior to authorization adequate in the context of pre-authorization operation, particularly with respect to equipment on the Covered List? For example, our rules currently allow for the operation of certain unauthorized devices in certain circumstances for purposes of demonstrations at a trade show or an exhibition and "evaluation of performance and determination of customer assembly during developmental, design, or pre-production states."[297] Are either of these exceptions to the general prohibition warranted for covered equipment? Should the Commission instead adopt different exceptions, such as for testing and product development, as we did for our import and marketing rules?[298] What additional categories or clarifications should the Commission consider? Do the existing provisions adequately balance the need to prevent harmful interference with the need to enable innovation, testing,

[296] 47 CFR § 2.805.

[297] 47 CFR § 2.805(d)(2).

[298] See infra para. 134.

and early-stage evaluation of new RF technologies? Commenters are invited to identify specific rule parts that may be overly restrictive or insufficiently protective.

L. UAS and Router Covered List definitions – "produced in a foreign country," "UAS critical components," "routers"

178. In the recent UAS, UAS critical components, and routers updates to the Covered List, the Commission has received numerous public inquiries regarding the definitions of "produced in a foreign country," "UAS critical components," and "routers." The Commission has provided some guidance answering these questions in Frequently Asked Questions (FAQs) posted to its website,[299] but the Commission believes it might be in the public interest to have codified definitions in its rules.

179. First, we seek comment on how best to interpret "produced in a foreign country" when used in a national security determination. For example, should the Commission interpret "produced in a foreign country" to include any equipment that does not qualify as a "domestic end product" as defined in 48 CFR 25.101(a)(1). Under 48 CFR 25.101(a)(1), for an end product to be considered a "domestic end product," the article must be manufactured in the United States and the cost of domestic components must exceed a certain percentage of the total cost of the finished product (currently set at 65%).[300] Specifically, we propose to interpret "produced in a foreign country" to mean "does not meet the 'domestic end product' standard." That is, those devices that are not both manufactured in the United States and that do not satisfy the specified thresholds for the cost of domestic components would be considered "produced in foreign country." We also take note of our past statement that production "includes … any major state of the process by which a device comes into existence" and includes the design and development of the device,[301] as well as the most recent router National Security Determination, which similarly stated that "[p]roduction generally includes any major stage of the process through which the device is made, including manufacturing, assembly, design, and development."[302] We therefore propose to further interpret "produced in a foreign country" to broadly include devices where design or development occurs foreign country. Thus, going forward we propose to interpret "produced in a foreign country" to mean a device that is *either* not a "domestic end product" or designed or developed in a foreign country.

180. We seek comment on this interpretation. We seek comment on whether this interpretation appropriately advances the intended statutory and policy objectives related to domestic sourcing, while providing clear, workable standards for industry. Should we add further clarity to the terms "design" and "development"? How should we interpret these terms? For example, should we draw from existing definitions in the CFR?[303] Should we adopt other definitions? We encourage commenters to provide ideas. Should the Commission find that if a certain number or percentage of foreign-based employees work on the design or development of the device, that device would be considered to have been "produced in a foreign country"? What would this number or percentage be? Would employing any foreign-based employee on design or development of a device render that device "produced in a foreign

[299] Federal Communications Commission, *Covered List FAQs: UAS and UAS Critical Components*, https://www.fcc.gov/covered-list-faqs-uas-and-uas-critical-components. (Last visited June 30, 2026); Federal Communications Commission, *FAQs on Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries*, Updated May 12, 2026, https://www.fcc.gov/faqs-recent-updates-fcc-covered-list-regarding-routers-produced-foreign-countries.

[300] 48. CFR § 25.101(a). For the manufactured end products, the domestic-component cost must exceed 60 percent of the cost of all the components, increasing to 65 percent for items delivered in 2024-2028, and 75 percent beginning in 2029, subject to exceptions for certain Commercially Available Off-the-Shelf (COTS) items.

[301] *Second Further Notice* at para. 53.

[302] Routers National Security Determination at 2.

[303] Should we, for instance, define "development" to mean "the systematic use of the knowledge or understanding gained from research, directed toward the production of useful materials, devices, systems or methods, including design and development of prototypes and processes," as defined by the Federal Highway Administration? 23 CFR § 420.203.

country?"

181. We note that subsequent to the addition of UAS and UAS critical components produced in a foreign country to the Covered List, DoW provided a time-bound exemption for UAS and UAS critical components that qualify as "domestic end products" as defined in 48 CFR 25.101(a)(1), which requires assembly in the United States and, for now, at least 65% of the components sourced from the U.S.[304] This would seem to suggest that DoW believed that at least some subset of UAS or UAS critical components that *are* domestic end products are nonetheless "produced in a foreign country" or the exemption would have been redundant. Therefore, should the Commission adopt a broader interpretation of "produced in a foreign country"? For example, should the Commission consider any device "produced in a foreign country" if the device would not be considered "Made in the United States" under Federal Trade Commission rules, i.e. "produced in a foreign country" "unless the final assembly or processing of the product occurs in the United States, all significant processing that goes into the product occurs in the United States, and all or virtually all ingredients or components of the product are made and sourced in the United States."[305] Alternatively, should the Commission adopt a narrower interpretation? For example, should the Commission adopt an interpretation based on trade law's concept of rule of origin?

182. We seek comment on whether whatever interpretation the Commission adopts should be applied to all determinations regarding existing and future production by location-based entries on the Covered List that use the language "produced in a foreign country".

183. Based on the description above, we also seek comment on whether to further refine, expand, or limit the scope of "UAS critical components." We seek comment to ensure that the definition of "UAS critical components" is sufficiently clear and consistently applied, and that it supports accurate compliance with the "domestic end product" requirements. As stated in the December 22, 2025 Covered List Public Notice, the term "UAS" critical components includes, but is not limited to the following UAS components and any associated software: (1) Data Transmission Devices; (2) Communications systems; (3) Flight controllers; (4) Ground control stations and UAS controllers; (5) Navigation systems; (6) Sensors and Cameras; (7) Batteries and Battery Management Systems; (8) and Motors.[306] This definition was provided in a National Security Determination from an Executive Branch interagency body, which included participation from several appropriate national security agencies.

184. The Commission noted in an FAQ that the Commission "understands 'UAS critical components' to mean components designed and intended primarily for use in UAS. For example, a camera with many potential functions and uses that could theoretically be attached to a drone is not a UAS critical component and so can receive FCC equipment authorization. But a camera designed and intended primarily to be a drone camera is a UAS critical component."[307] Should the Commission codify this definition? Should the Commission adopt a different definition that better tracks the National Security Determination's intention?

185. The Commission also seeks comment on codifying a definition of "routers" for purposes of the Covered List. In the March 20, 2026 National Security Determination, the term "Routers" was defined by the National Institute of Science and Technology's Internal Report 8425A to include "consumer-grade networking devices that are primarily intended for residential use and can be installed by the customer. Routers forward data packets, most commonly Internet Protocol (IP) packets, between

[304] Federal Communications Commission, Fact Sheet: FCC Updates Covered List to Exempt Certain Drones from Restrictions, Releases Additional FAQs, Jan. 7, 2026, https://docs.fcc.gov/public/attachments/DOC-417528A1.pdf.

[305] 16 CFR § 323.2.

[306] *Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List*, WC Docket 18-89, Public Notice, DA 25-1086 (Dec 22, 2025)

[307] Federal Communications Commission, *Covered List FAQs: UAS and UAS Critical Components*, https://www.fcc.gov/covered-list-faqs-uas-and-uas-critical-components. (Last visited June 30, 2026).

networked systems."[308] The Commission adopted that same definition in its Routers Public Notice and FAQs, more explicitly finding that a device is a router if the following elements are present: (1) it is a consumer-grade networking device that is primarily intended for residential use; (2) it can be, but is not required to be, installed by the customer; and (3) it forwards data packets, most commonly Internet Protocol (IP) packets, between networked systems.[309]

186. The Commission, relying on its technical expertise and experience, clarified in the FAQs that the following devices all constitute a consumer-grade router: consumer or small and medium-sized business routers sold or rented through retail and self-installable by end users; consumer-grade portable or mobile MiFi Wi-Fi or hotspot devices for residential use; LTE/5G CPE devices for residential use; residential routers installed by a professional or ISP; and residential gateways that combine modem and router functions.[310] Similarly, we also distinguished that the following devices are not considered a consumer-grade routers: Analog Telephone Adapters ("ATAs") that include Ethernet LAN and WAN ports; femtocells; Optical Network Terminals (ONTs); industrial, enterprise, or military equipment; and mobile phones with hotspot features.[311]

187. We seek comment on whether to further refine, expand, or limit the scope of how we have defined "Routers." Should we add further detail to this definition, such as clarifying whether additional specific devices are or are not "routers"? Are additional measures necessary to ensure that the definition of "routers" is sufficiently clear, consistently applied, and accurately reflects the National Security Definition? What other clarifications to the inclusions or exclusions are necessary? We invite comment generally on this point.

M. Term limits on equipment authorizations

188. In the *Second Further Notice*, we sought comment on whether equipment authorizations should have an expiration date or be term limited.[312] Currently, equipment certifications remain valid indefinitely unless they are withdrawn, revoked, or terminated or become subject to a subsequent rule change that affects their validity. We believe that there may be significant value to the automatic expiration of an authorization and seek additional comment from consumers and the industry. Specifically, we seek comment on the various supply chain effects if the Commission were to uniformly impose an expiration date on all equipment authorizations, with prospective effect. Should the Commission adopt such a rule? Should such a rule be limited to the marketing of equipment, or would it also apply to its continued operation? Is a ten-year period adequate?

189. Different classes of equipment have different lifecycles, after which equipment producers typically cease issuing software and security updates. With certain consumer equipment expected to last less than five years, would a ten-year limit permit most consumer or enterprise equipment to age out naturally? Covered List equipment would be ineligible for a new authorization, but should other term-expired equipment be permitted to renew automatically or by grant of a renewal application submitted to the Commission? If the Commission adopts rules setting term limits on equipment authorizations, what specific requirements should the Commission adopt for the renewal process in order to balance the burdens on the applicant, the industry, and the agency? Should the Commission adopt comparable requirements to the initial equipment authorization, or should the Commission adopt more streamlined

[308] National Institute of Standards and Technology, U.S. Department of *Commerce. Recommended Cybersecurity Requirements for Consumer-Grade Router Products*, NIST IR 8425A, including Appendix C ("Consumer-Grade Acquisition Scenarios Discussion"), Sept. 2024, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8425A.pdf

[309] *See* Routers FAQs, https://www.fcc.gov/faqs-recent-updates-fcc-covered-list-regarding-routers-produced-foreign-countries.

[310] *Id.*

[311] *Id.*

[312] 2d FNPRM at para. 91.

requirements

190. The Commission expects to continually advance the development of new communications equipment and so also expects to refine its equipment authorization rules. Accordingly, should there be an expedited application and approval process instead of automatic renewals? If so, which equipment authorization procedures should be streamlined, or developed, to speed future authorization renewals and reduce associated costs? Are there parallels from spectrum licensing that should be integrated into the equipment authorization and renewal processes? How should the expiration of an equipment authorization apply to SDoC equipment? We seek any and all comments in this regard.

N. Registration of SDoC devices

191. The SDoC process was "originally established to reduce the burden on manufacturers of Class B personal computers and peripherals by eliminating the delays resulting from the requirement to obtain a Commission approval prior to marketing equipment."[313] At that time, the Commission concluded that it was not "necessary to mandate the automatic filing of information with the Commission," because "as long as the measurement procedures are properly followed and testing is performed by a competent laboratory…filing of information with the FCC would not provide any added assurance of compliance and would create an unnecessary administrative burden."[314] The Commission also noted the limitations of its databases at the time, including that the FCC Public Access Link system, organized around FCC ID numbers, could not support storing SDoC information.[315]

192. As the equipment authorization system has evolved, and threats to our national security have increased with the proliferation of insecure equipment by bad actors, the assumptions underlying the SDoC framework no longer hold. The Commission can no longer presume that measurement procedures are consistently followed or that testing is conducted by competent laboratories. In the past year, we have taken action to remove 28 entities from the equipment authorization system due to improper conduct or because they posed unacceptable risks to national security. The Commission's information-management capabilities have also changed markedly. We no longer rely on physical publications such as the Radio Equipment List, and we now maintain multiple databases capable of handling the information relevant to SDoCs and related authorizations. Additionally, given the new national security function that the FCC's equipment authorization has taken on in the wake of the Secure Networks Act, the Secure Equipment Act, and our corresponding rules, it is vital that the Commission have greater oversight over devices that receive authorization through SDoC to protect national security from dangerous devices. For example, as noted above,[316] covered equipment is prohibited from receiving equipment authorization, even through SDoC, and entities identified on the Covered List are similarly prohibited from utilizing the SDoC process. Given these substantial changes, we are revisiting our 1996 determination not to require registration of SDoC-authorized devices.

193. We therefore propose to require that all devices authorized through the SDoC process be registered with the Commission with a unique identification number, which the Commission will publicly list on its website, comparable to the oversight and transparency of the certification process and FCC IDs. We seek comment on the appropriate mechanism for such registration. What existing databases or systems could support SDoC registrations while minimizing burdens on suppliers? What specific information should an SDoC registration include? Should it include sufficient information for the Commission to be able to identify the type of device? Should it include any of the information that is required through the certification process, including any of the information that the Commission seeks

[313] *In the Matter of: Amendment of Part 15 and other Parts of the Commission's Rules*, Notice of Proposed Rulemaking and Order. ET Docket 01-278. October 2, 2001.

[314] *In the Matter of: Amendment of Parts 2 and 15 of the Commission's Rules to Deregulate the Equipment Authorization Requirements for Digital Devices. Report and Order*. ET Docket No. 95-19. May 9, 1996.

[315] *Id.* at fn. 12.

[316] See supra at paras. 157-158.

comment on requiring in this *Further Notice*, such as HBOM and SBOM information?[317] Should a unique SDoC registration identifier be displayed on the device label? We also seek comment on the appropriate scope of this requirement. Should it apply to all SDoC devices, only those falling within a Covered List sector, or to some other subset? Should the Commission require all composite devices (i.e. those that include both certified and SDoC elements) to be listed in a particular way so it is obvious what certified equipment and what equipment authorized by SDoC is combined? Should SDoC documentation be available through the database? Finally, we seek comment on what enforcement mechanisms or procedures the Commission should adopt to ensure effective oversight of SDoC registrations.

194. In the *Third Report and Order*, we adopted rules that clarify that the term "marketing" applies to online marketplaces as a means of significantly curtailing the marketing of unauthorized equipment.[318] We also adopted rules that require that online marketing materials for certified equipment must provide consumers with the device's FCC ID.[319] We seek comment on whether similar rules should apply to radio frequency devices authorized pursuant to SDoC. Pursuant to sections 2.1074 and 2.1077, every device that is authorized by an SDoC must include a compliance information statement at the time of marketing or importation that also identifies the party responsible for compliance and the unique product name and model number.[320] This information is, thus, readily available to every supply chain entity that physically manages the equipment. We acknowledge that many online marketplaces will not physically manage or involve themselves in the distribution of every product that is offered on their platforms; nevertheless, these entities are in a far superior position to be able to obtain this information from the supplier or manufacturer. It is also critical to the safety of U.S. consumers and communications networks that equipment authorizations are verified prior to being offered for sale.

195. Thus, we propose that, for radio frequency devices not authorized by certification, online marketplaces collect and take reasonable steps to verify the SDoC compliance information statement or a statement that the radio frequency device to be marketed does not require an FCC authorization and also meets any applicable technical standards.[321] We believe that displaying equipment authorization information in the online advertisement may be the single most effective means by which the Commission, consumers, supply chain entities, competitors, and other stakeholders may verify whether a particular device may lawfully be marketed within the United States. We seek comment on viability, benefit, additional expenses that may be incurred, and any other factors relevant to the proposed new requirement. What issues might online marketplaces encounter while obtaining authorization information, verifying its accuracy, or displaying this information online? The compliance information statement may take up valuable real estate on the product listing page. Would providing a URL or QR code that links to the full SDoC compliance statement provide a viable, secure and valid alternative? What other means might be used to provide the consumer with valuable compliance information at the time of marketing? What types of information do online marketplaces already collect regarding third party retailers and the products that they market to U.S. consumers? Would publication of an SDoC or compliance statement create any unfair competitive advantage or disadvantage? Are additional changes to the SDoC rules needed for online marketplaces to assess the validity of an SDoC? We further propose that any compliance information obtained and displayed by online marketplaces must match the product that is being advertised. If we adopt rules requiring registration for SDoC-authorized devices, how might we modify this proposal? For example, if the FCC adopts a registration requirement for SDoC devices, should we require online marketplaces display SDoC registration numbers for any device sold on their

[317] *See, supra* at paras. 121-122.

[318] *See, supra* at para. 28; The Commission also clarifies that e-commerce platforms that list third-party products on their platforms are engaged in marketing, because they are engaged in the "offer for sale" of these products. …]

[319] *See, supra* at paras. 50-53.

[320] 47 CFR §§ 2.1074, 2.1077.

[321] For example, certain devices are excepted from authorization—whether certification or SDoC—as long as they meet certain technical criteria. *See* 47 CFR § 15.103.

platforms, as we required for FCC IDs above.[322]

O. Data Analytics Capability and need for modern EAS database

196. Many public commenters have urged the FCC to modernize the Equipment Authorization System (EAS) database.[323] We seek comment on such suggestions. What features would be helpful in the Commission's effort to modernize the EAS system, both to support the FCC's national security priorities while also streamlining and alleviating administrative burden on our TCB partners and other participants in the equipment authorization process? What, if any, changes to the information collection would be helpful, and what portions of the process can be streamlined or done in a more parallel fashion? How can we better share information and other data with stakeholders? We welcome all comments and proposals with estimates on associated benefits and costs.

P. Submarine Cables

197. In the *2025 Submarine Cable First Report and Order*,[324] the Commission adopted new certifications and routine conditions that will require applicants and cable landing licensees to comply with Covered List requirements. Specifically, we adopted rules requiring that, as a condition of a potential grant of an application for a cable landing license, applicants must certify that their submarine cable system will not use equipment or services identified on the Covered List.[325] We also adopted a requirement that, as a condition of a potential grant of an application to modify a cable landing license to add a new segment, applicants must certify that the new submarine cable segment and landing point will not use equipment or services identified on the Covered List.[326] In addition, we adopted a rule requiring existing cable landing licensees, with certain exceptions, to certify that they will not add covered equipment or services to their submarine cable system under the license.[327]

---

[322] *See supra* paras. 53-60.

[323] *See, e.g.* Connor Healy, Director Government Research, IPVM, *Modernizing FCC Databases Can Put Valuable Information in Public Hands While Assisting the FCC in Protecting National Security*. June 5, 2024. https://s.ipvm.com/uploads/embedded_file/d223c17161ef12ad6103ab23e32801512973c23f792812e9f7f0f68748188f82/51612351-a304-4792-89b0-db1cae328409.pdf.

[324] *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks*, OI Docket No. 24-523, MD Docket No. 24-524, Report and Order and Further Notice of Proposed Rulemaking, 40 FCC Rcd 6481 (2025) (*2025 Submarine Cable First Report and Order and FNPRM)*; corrected by Erratum, https://docs.fcc.gov/public/attachments/DOC-414544A1.pdf (OIA and OMD Sept. 16, 2025); corrected by Second Erratum, https://docs.fcc.gov/public/attachments/DOC-415107A1.pdf (OIA and OMD Oct. 24, 2025) (*2025 Submarine Cable First Report and Order*); Cable Landing License Act of May 27, 1921, Pub. L. No. 8, 67th Cong., ch. 12, § 1, 42 Stat. 8 (1921) (codified as amended at 47 U.S.C. §§ 34-39); Exec. Order No. 10,530, 19 Fed. Reg. 2709, § 5(a) (May 12, 1954), *reprinted as amended in* 3 U.S.C. § 301.

[325] *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6548-50, 6641-42, 6634, para. 125-126, Appx. A (§§ 1.70006(d), 1.70007(u)); *see 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*, Second Report and Order and Second Further Notice Of Proposed Rulemaking, FCC-xx (x, x, 2026) (*2026 Submarine Cable Second Cable Report and Order*) (amending section 1.70007(u) to incorporate new routine conditions and further restructure section 1.70007(u)(1) to improve regulatory clarity).

[326] We adopted a rule that a licensee whose modification application to add a new segment is filed and granted after the effective date of the *2025 Submarine Cable First Report and Order* shall not use equipment or services identified on the Covered List on the new segment and the new landing point. *See id.* at 6550, 6634, para. 128, Appx. A (§ 1.70007(u)(1)).

[327] *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6548-49, 6634, 6551-53, 6654, paras. 125, 131-134, Appx. A (§ 1.70023) (stating, "this condition shall not apply to a licensee that is identified on the Covered List (continued….)

198. We propose to narrow and more clearly define the scope of certain submarine cable rules in light of subsequent updates to the Covered List to only prohibit applicants and licensees from using or adding Covered List equipment and services from the producer/provider-based determinations rather than the production location-based determinations, unless a location-based determination specifically refers to the equipment or services at issue posing national security threats when used in submarine cable systems. We propose that PSHSB, when it updates the Covered List, would determine whether submarine cable licensees would be subject to any future location-based determination, based solely on the content of the determination itself.

199. Since the adoption of the *2025 Submarine Cable First Report and Order*, the Commission updated the Covered List based on specific determinations made by an Executive Branch interagency body with appropriate national security expertise,[328] regarding the unacceptable risks posed by UAS, UAS critical components, and routers produced in foreign countries.[329] As discussed above, these were the first instances where a specific determination identified equipment and services produced in foreign countries, a production location-based determination, rather than equipment or services produced or provided by specific entities, a producer/provider-based determination.[330] Additionally, in the *2026 Submarine Cable Second Report and Order*, we adopted a certification and a routine condition that broadly prohibits the use or addition of any principal equipment on the submarine cable system that is produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in section 1.70001(g).[331] For purposes of our submarine cable licensing rules, we tentatively conclude that tailoring the Covered List certification requirements and routine conditions by relying on producer/provider-based determinations, rather than prohibiting the use or addition of production location-based determinations would be consistent with our original intent in the *2025 Submarine Cable First Report and Order* and provide greater regulatory certainty and minimize burdens.[332] At the same time, we believe this proposed approach, in combination with other application rules, certification requirements, and routine conditions adopted in the *2025 Submarine Cable First*

whose cable landing license was or is granted prior to" the effective date of the rule). Section 1.70023 requires licensees to submit this certification within sixty (60) days of the effective date of the rule. *Id.*

[328] 47 U.S.C. § 1601(c); 47 CFR § 1.50001(e) ("The term 'determination' means any determination from sources identified in § 1.50002(b)(1)(i)-(iv) that communications equipment or service pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."); 47 CFR § 1.50002(b).

[329] *See supra,* para. 10.

[330] *Id.*

[331] *2026 Submarine Second Cable Report and Order* at [x]; 47 CFR § 1.70001(g). Licensees whose application for a cable landing license is filed and granted after the effective date of the *2026 Submarine Cable Report and Order* must ensure that no such principal equipment is used or added, whether by the licensee or any other entity, on their licensed submarine cable system. *2026 Submarine Cable Report and Order* at x. Existing licensees must ensure that no such principal equipment is added, whether by the licensee or any other entity, on their licensed submarine cable system. *Id.*

[332] Consistent with this proposed approach, we do not propose to modify those Covered List requirements adopted in the *2025 Submarine Cable First Report and Order* that rely on producer/provider determinations. *See, e.g.*, 47 CFR § 1.70004(a)(ii) ("The disqualifying condition will presumptively preclude the grant of an application, as specified in paragraph (a)(2) of this section, filed by any applicant . . . That is identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601-1609"); *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6639, 6653, Appx. A (§§ 1.70005(g) (requiring in an initial application for a cable landing license "[a] statement disclosing whether or not the applicant uses and/or will use the following third-party service providers, as defined in § 1.70001(d), in the operation of the submarine cable system . . . [a]ny entity identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601-1609"), 1.70017(b) (applying the Foreign Adversary Annual Report requirement to a licensee "[t]hat is identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601-1609")).

Report and Order[333] and *2026 Submarine Cable Second Report and Order*[334] would continue to protect critical submarine cable infrastructure against foreign adversary and other threats.

200. *Producer/Provider-Based Covered List Certifications for Applications and Routine Conditions*. We propose to amend section 1.70006(d) by requiring applicants for initial cable landing licensee applications to certify, as a condition of a potential grant, that their submarine cable system will not use equipment or services that are identified on the Covered List in the producer/provider category.[335] Accordingly, we propose to amend the routine condition in section 1.70007(u)(1) by prohibiting a licensee, whose application is filed and granted after the effective date of the *2025 Submarine Cable First Report and Order*, from using such covered equipment or services on its submarine cable system under the license.[336] We also propose to amend section 1.70007(u)(1)(i) by prohibiting a licensee, whose modification application to add a new segment is filed and granted after the effective date of the *2025 Submarine Cable First Report and Order*, from using such covered equipment or services on the new segment and the new landing point.[337] Consistent with this proposed change, a licensee seeking a modification of its license under section 1.70011(a) would be required to certify that it accepts and will abide by the routine conditions in section 1.70007, as amended in this proceeding.[338]

201. *Producer/Provider-Based Covered List Routine Conditions for All Licensees*. We propose to amend section 1.70007(u) by prohibiting a cable landing licensee from adding to its submarine cable system equipment or services that are identified on the Covered List in the producer/provider category, or other a location-based entry when the determination makes specific reference to national security threats that are specific to submarine cable systems, while retaining the current exception for existing licensees that are entities identified on the Covered List.[339] We note that our proposals in this

[333] *See generally 2025 Submarine Cable First Report and Order*.

[334] *See generally 2026 Submarine Cable Second Report and Order*.

[335] *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6641-42, Appx. A (§ 1.70006(d)) ("An applicant must certify to the following in the initial application for a cable landing license . . . That the submarine cable system will not use *equipment or services identified on the Covered List* that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601 through 1609.") (emphasis added).

[336] *Id.* at 6634, Appx. A (§ 1.70007(u)); *2026 Submarine Cable Second Report and Order* at 6634, Appx. A (§ 1.70007(u))(1)) ("A licensee whose application for a cable landing license is filed and granted after November 26, 2025, shall not use *equipment or services identified on the Covered List* on its submarine cable system under the license.") (emphasis added).

[337] *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6634, Appx. A (§ 1.70007(u)(1)); *2026 Submarine Cable Second Report and Order* at 6634, Appx. A (§ 1.70007(u)(1)(i)) ("A licensee whose modification application to add a new segment is filed and granted after November 26, 2025, shall not use *equipment or services identified on the Covered List* on the new segment and the new landing point.") (emphasis added).

[338] *See 2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6647, Appx. A (§ 1.70011(a)(2)) (requiring that an application to add a landing point(s), segment(s), or other like material changes to a submarine cable system must also include certifications set forth under § 1.70006, except for § 1.70006(d)); *id.* at 6641, Appx. A (§ 1.70006(a)) (requiring a certification that the applicant accepts and will abide by the routine conditions specified in § 1.70007). Consistent with the overall changes proposed, other applications and reports subject to subpart FF of the rules would similarly require a certification that the applicant or licensee accepts and will abide by the routine conditions in section 1.70007, as amended in this proceeding. *See id.* at 6647, 6651-52, 6653-54, Appx. A (§§ 1.70011(b)(4), 1.70012(b)(7), 1.70013(b)(8), 1.70017(c)(2), 1.70020(b)) (requiring certifications set forth under § 1.70006, as specified therein, or that it accepts and will abide by the routine conditions specified in § 1.70007); *2026 Submarine Cable Second Report and Order* at 6653-54, Appx. A (§ 1.70018(c) (requiring a certification that the licensee accepts and will abide by the routine conditions in § 1.70007).

[339] *Id.* at 6634, Appx. A (§ 1.70007(u)(1)); *2026 Submarine Cable Second Report and Order* at 6634, Appx. A (§ 1.70007(u)) ("No licensee shall add to its submarine cable system(s) under its respective license(s) *equipment or services identified on the Covered List* that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. §§ 1601-1609; except, this part of paragraph (u) shall not apply to a licensee that is

(continued….)

Further Notice will not alter licensees' obligation to submit the certification required in section 1.70023 once that rule is effective.[340]

202. We seek comment on these proposals. We seek comment on the impact of these proposals on applicants and licensees. Would narrowing the scope of the Covered List certification requirements and routine conditions to "producer/provider-based determinations" create national security vulnerabilities and other risks for submarine cable infrastructure? We also seek comment on including the application of these Covered List certification requirements and routine conditions to location-based additions to the Covered List where the specific determination at issue specifically references national security threats in the context of submarine cable systems. We seek comment on the costs and benefits of these proposals and alternative approaches. The Commission previously adopted a rule requiring applicants for a cable landing license to certify, as a condition of a potential grant, that their submarine cable systems will not use equipment or services identified on the Covered List. By clarifying that this requirement—established in the submarine cable proceeding—is limited to producer or provider-based Covered List determinations and does not extend to production location-based criteria except where the determination specifically references threats in the context of submarine cable systems, the Commission aims to eliminate any potential ambiguity in interpreting the certification obligation. Since the clarification removes regulatory burdens, we tentatively conclude that this clarification will reduce implementation costs and improve regulatory certainty. We seek comment on this tentative conclusion.

Q. U.S.-based Liable Party for FCC-certified equipment

203. Currently, the party legally responsible for compliance associated with SDoC-authorized equipment must be located in the United States (i.e., the responsible party).[341] Our rules do not, however, require the party legally liable for *certified* equipment to be located in the United States. Instead, in general, the grantee or manufacturer is responsible for compliance associated with certified equipment, unless the equipment was modified by another party. [342] Because of this, many liable parties for certified equipment are located outside of the United States. As a result, the Commission may not always be able to communicate timely with foreign liable parties for certified equipment, and the Commission's attempts to enforce compliance by foreign liable parties for certified equipment have sometimes been hindered.[343] In the *First Report and Order*, we revised our rules to require that each applicant for equipment certification designate a U.S. agent for service of process.[344] In the *NPRM* and the *First Further Notice,* we proposed going further and requiring a U.S.-based liable party for FCC-certified equipment, analogous to the existing requirement that an SDoC liable party be located in the United States. Under the SDoC approach, the responsible party must be located in the United States and, depending on the circumstances, could be the manufacturer or assembler, the importer, or the retailer. Specifically, if the manufacturer or assembler is not located in the United States and the equipment is imported, the importer would become the new responsible party.[345]

204. In response to the *NPRM,* commenter Hytera US supported identification of a U.S.-based

identified on the Covered List whose cable landing license was or is granted prior to November 26, 2025.") (emphasis added).

[340] *2025 Submarine Cable First Report and Order*, 40 FCC Rcd at 6548-49, 6634, 6551-53, 6654, paras. 125, 131-134, Appx. A (§ 1.70023).

[341] 47 C.F.R. § 2.909(b).

[342] *First Further Notice,* paras. 312-316; *compare* 47 CFR § 2.909(a) *with* 47 CFR § 2.909(b).

[343] *See, e.g., In the Matter of Eken Group Limited,* Notice of Apparent Liability for Forfeiture, 39 FCC Rcd 12990 (2024) (FCC 24-122, released November 21, 2024) (Eken NAL).

[344] *First Report and Order* at para. 59.

[345] 47 CFR 2.909(b)(2)

liable party.[346] Otherwise, the Commission has received no comment on this issue.

205. We propose to require a U.S.-based liable party for FCC-certified equipment to strengthen enforcement of our rules and promote regulatory harmonization by aligning our equipment certification requirements with SDoC requirements. Although we imposed a requirement to designate a U.S. agent for service in the *First Report and Order,* we have found in our experience that requirement to be insufficient to ensure compliance with our rules. Since implementing the U.S. agent for service of process requirement in our rules,[347] we have found that certification applicants have, in multiple instances, provided false names and addresses for the U.S. agent for service of process, allowing bad actors to evade enforcement efforts by placing them beyond the reach of U.S. law.[348] We tentatively conclude that this gives foreign actors an unfair advantage in the marketplace. U.S.-based equipment manufacturers and grantees are subject to U.S. law, and if their products harm U.S. consumers, they can be held accountable under the Commission's enforcement authority because their documents, witnesses, and financial assets are within reach of U.S. law. This is not always the case for foreign actors; we have seen many instances of such actors evade the Commission's enforcement authority despite the requirement to designate a U.S. agent for service of process.[349]

206. We propose to adopt the requirement that every applicant or grantee for FCC-certified equipment have a U.S.-based liable party and revise our equipment certification rules in section 2.909(a) of our rules to align with the SDoC rules in section 2.909(b). If revised rules were adopted, the liable party would be (1) the manufacturer or assembler, if located in the United States, (2) the importer(s) if the equipment is imported, (3) the retailer or other entity assuming the liable party function pursuant to an agreement with the manufacturer, assembler, or importer, or (4) if the equipment modified without authority of the liable party, the party performing the modification if located in the United States, or the importer if imported subsequent to modification.

207. Under this proposal, each potential liable party, including the importer, would be jointly and severally liable with the foreign grantee for violations of the Communications Act or of our rules. A U.S.-based liable party must have organizational authority to ensure compliance and cooperation with enforcement investigations. This includes the ability to produce documents, relevant witnesses, and financial assets in the United States to support enforcement investigations. Because importers or other entities would assume the role of the U.S.-based liable party if grantees are not based in the United States and the equipment is imported, this requirement would ensure that financial assets are available for enforcement purposes.[350] If a U.S.-based liable party was unable to ensure compliance by the foreign grantee, the Commission could seek sanctions or initiate revocation proceedings against the grantee. This could also include, for example, making adverse inferences to support revocation of equipment authorizations and disqualifying U.S.-based liable parties that do not comply with our rules.

208. If revised rules are adopted, we would intend to enforce this requirement as needed and expect grantees and their U.S.-based liable parties to respond promptly to Commission inquiries regarding

[346] Hytera US Comments at 13.

[347] *See* 47 C.F.R. § 2.911(d)(7) (effective February 6, 2023).

[348] *See, e.g.,* Eken NAL.

[349] *Id.*

[350] We also note that the INFORM Consumers Act, 15 U.S.C. § 45f, requires online marketplaces to collect, verify, and disclose identification and financial information for high-volume third-party sellers and generally make that information available to consumers in a clear and conspicuous manner. These requirements will make it easier to identify financial assets within reach of our enforcement authority and will strengthen our ability to enforce the Communications and our rules against those actors who benefited from the marketing, sale, or importation of non-complaint equipment.

the U.S.-based liable party.[351] Failure to respond could result in initiation of revocation proceedings against the grantee.

209. We seek comment on these proposals. We seek comment on the impact of these proposals on grantees, manufacturers, importers, and retailers. We seek comment on the costs and benefits of these proposals and alternative approaches.

V. PROCEDURAL MATTERS

210. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),[352] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[353] Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this Report and Order on small entities. The FRFA is set forth in Appendix C.

211. The Commission has also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of the rule and policy change proposals on small entities in the Second Further Notice of Proposed Rulemaking. The IRFA is set forth in Appendix D. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the Further Notice indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

212. *Paperwork Reduction Act*. This document contains proposed new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law No. 10413. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on any information collection requirements contained in this document. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107198, see 44 U.S.C. § 3506(c)(4), we seek specific comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

213. *Ex Parte Presentations—Permit-But-Disclose*. The proceeding this Further Notice of Proposed Rulemaking initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[354] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In

[351] Such inquiries are exempted from the information collection requirements of the Paperwork Reduction Act to the extent such information is collected during the conduct of an administrative action or investigation involving an agency against specific grantees.

[352] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[353] 5 U.S.C. § 605(b).

[354] 47 CFR § 1.1200 *et seq.*

proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

214. *Providing Accountability Through Transparency Act.* Consistent with the Providing Accountability Through Transparency Act, Public Law 1189, a summary of this document will be available on https://www.fcc.gov/proposedrulemakings.

215. *OPEN Government Data Act*. The OPEN Government Data Act[355] requires agencies to make "public data assets" available under an open license and as "open Government data assets," *i.e.*, in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization.[356] This requirement is to be implemented "in accordance with guidance by the Director" of the OMB.[357] The term "public data asset" means "a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)]."[358] A "data asset" is "a collection of data elements or data sets that may be grouped together,"[359] and "data" is "recorded information, regardless of form or the media on which the data is recorded."[360]

- *Filing Requirements—Comments and Replies*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. All filings must be addressed to the Secretary, Federal Communications Commission.
    - Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.

[355] Congress enacted the OPEN Government Data Act as Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202.

[356] 44 U.S.C. §§ 3502(20), (22) (definitions of "open Government data asset" and "public data asset"), 3506(b)(6)(B) (public availability).

[357] OMB has not yet issued final guidance.

[358] 44 U.S.C. § 3502(22).

[359] 44 U.S.C. § 3502(17).

[360] 44 U.S.C. § 3502(16).

- Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.

216. *People with Disabilities*. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

217. *Congressional Review Act*. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, has found, and the Commission concurs, that this rule is "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this Third Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

218. *Further Information*. For further information, contact the Office of Engineering and Technology, at EASecurity3@fcc.gov.

VI. ORDERING CLAUSE

219. IT IS ORDERED, pursuant to the authority found in sections 4(i), 301, 302, 303, 403, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 301, 302a, 303, 403, 503; the Cable Landing License Act, 47 U.S.C. §§ 34-39; the Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. §§ 1601-1609; and the Secure Equipment Act of 2021, Pub. L. 117-55, 135 Stat. 423, 47 U.S.C. § 1601 note, that this Third Report and Order and Third Further Notice of Proposed Rulemaking IS HEREBY ADOPTED.[361]

220. IT IS FURTHER ORDERED that the rule amendments set forth in Appendix [A] of this Third Report and Order SHALL BE EFFECTIVE 30 days after publication in the Federal Register, except for those amendments in para. 38 and [rule section], which SHALL BE EFFECTIVE as of adoption of this Third Report and Order.

221. IT IS FURTHER ORDERED that the Commission's Office of the Secretary SHALL SEND a copy of this Third Report and Order and Third Further Notice of Proposed Rulemaking, including the Final and Initial Regulatory Flexibility Analyses, to the Chief Counsel of the Small Business Administration Office of Advocacy.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[361] Pursuant to Executive Order 14215, 90 Fed. Reg. 10447 (Feb. 20, 2025), this regulatory action has been determined to be significant under Executive Order 12866, 58 Fed. Reg. 68708 (Dec. 28, 1993).

APPENDIX A

Final Rules

For the reasons set forth, the Federal Communications Commission amends parts 1 and 2 of Title 47 of the Code of Federal Regulations as follows:

Part 1 — PRACTICE AND PROCEDURE

1. The authority citation for part 1 continues to read as follows:

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. 2461 note; 47 U.S.C. 1754, unless otherwise noted.

2. Amend § 1.50001 by:
   a. Adding new paragraph (f).
   b. Redesignating paragraph (f) as paragraph (e).
   c. Redesignating paragraph (e) as paragraph (g).
   d. Redesignating paragraphs (g) though (i) as paragraphs (h) through (j) to read as follows:

§ 1.50001 Definitions.

For purposes of this subpart:

* * * * *

(f) ***Critical Infrastructure***. For purposes of implementing section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232; 132 Stat. 1918), the term "critical infrastructure" has the meaning given in Section 5195c(e) in Title 42 of the U.S Code. This definition encompasses systems and assets used in the provision of services or functions in the 16 critical infrastructure sectors, as identified in National Security Memorandum 22 and further clarified by the Department of Homeland Security, to provide any of the 55 National Critical Functions published by the Department of Homeland Security through the National Risk Management Center.
For the reasons discussed in the document above, the Federal Communications Commission proposes to amend part 2 of Title 47 of the Code of Federal Regulations as follows:

Part 2 — FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

3. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336 unless otherwise noted.

4. Amend § 2.803 by adding a subparagraph to paragraph (a), redesignating existing paragraphs (c) and (d) as paragraphs (d) and (e) and adding paragraph (c) to read as follows:

§ 2.803 Marketing of radio frequency devices prior to equipment authorization.

(a) * * *

Marketing includes the listing of regulated equipment on an online marketplace, in combination with any of the following activities: consignment, warehousing, inventory

management, order processing, labelling, packaging, billing, or fulfilment services – even if that equipment is sold or offered for sale by a third-party seller.

* * * * *

(c) Online marketplaces marketing radiofrequency devices must ensure that information related to equipment authorization, including the associated FCC ID as set forth in § 2.925, is made available in online marketing materials at the time of sale.

* * * * *

5. Amend § 2.902 by adding following definitions to read as follows:

§ 2.902 Terms and Definitions.

Logic-bearing hardware component. Any device, system, module, sub-assembly, integrated circuit, or other physical component that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques; inclusive of telephone equipment that uses digital techniques or any device, system, module, sub-assembly, integrated circuit, or other physical component that generates and uses radio frequency energy for the purpose of performing data processing functions, such as electronic computations, operations, transformations, recording, filing, sorting, storage, retrieval, or transfer.

Online marketplace. An "online marketplace" as that term is defined in 15 USC § 45f(f)(4).

6. Amend § 2.903 by revising the title and revising paragraph (b) and (d) to read as follows:

§ 2.903 Prohibition on authorization of equipment on the Covered List and related equipment.

* * *

(b) All devices that incorporate one or more of the following components are prohibited from obtaining an equipment authorization under this subpart:

(1) Equipment meeting the descriptions in paragraph (a)(1) or (2) of this section; and

(2) A logic-bearing hardware component produced by an entity identified on the Covered List pursuant to § 1.50002 of this chapter if—had such entity produced the device itself, rather than just a component—the device would be prohibited from receiving authorization under paragraph (a).

* * * * *

(d) Each entity named on the Covered List as producing covered communications equipment, as established pursuant to § 1.50002 of this chapter, must provide to the Commission the following information: the full name, mailing address or physical address (if different from mailing address), email address, and telephone number of each of that named entity's associated entities (*e.g.,* subsidiaries or affiliates) identified on the Covered List as producing covered communications equipment.

(1) Each entity named on the Covered List as producing covered communications equipment must provide the information described in this section no later than March 8, 2023;

(2) Each entity named on the Covered List as producing covered communications equipment must provide the information described this section no later than 30 days after the effective date of each updated Covered List; and

(3) Each entity named on the Covered List as producing covered communications equipment must notify the Commission of any changes to the information described in this section no later than 30 days after such change occurs.

7. Amend § 2.932 by revising paragraph (a) by adding a second sentence and adding paragraph (f). to read as follows:

§ 2.932 Modification of equipment.

(a) A new application for an equipment authorization shall be filed whenever there is a change in the design, circuitry or construction of an equipment or device for which an equipment authorization has been issued, except as provided in paragraphs (b) through (d) of this section. The exceptions set forth in this section do not apply to changes made by Covered List entities or changes that would result in the modified device being considered covered communications equipment.

* * * * *

(f) Notwithstanding other provisions of this section, use of the permissive change procedures to modify equipment that is produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, is prohibited. Any modification to such equipment must be authorized under the equipment certification provisions under subpart J of this part.

8. Amend § 2.1043 by adding a sentence to the beginning of paragraph (a) and revising the following sentence to read as follows:

§ 2.1043 Changes in certificated equipment.

(a) Any changes made by Covered List entities or changes that would result in the modified device being considered Covered Equipment shall not be performed without application for and authorization of a new grant of certification. In all other instances, except as provided in paragraph (b)(3) of this section, changes to the basic frequency determining and stabilizing circuitry (including clock or data rates), frequency multiplication stages, basic modulator circuit or maximum power or field strength ratings shall not be performed without application for and authorization of a new grant of certification. Variations in electrical or mechanical construction, other than these indicated items, are permitted provided the variations either do not affect the characteristics required to be reported to the Commission or the variations are made in compliance with the other provisions of this section. Changes to the software installed in a transmitter that do not affect the radio frequency emissions do not require any additional filings and may be made by parties other than the holder of the grant of certification.

9. Amend **§** 2.1204 by adding “and” in paragraph (a)(2) and remove and reserve (a)(4)(iv) to read as follows:

§ 2.1204 Import conditions.

* * * * *

(a)(2) The radio frequency device is not required to have an equipment authorization and the device complies with FCC technical and administrative regulations.

* * *

(a)(4)(iv) [Reserved]

* * * * *

APPENDIX B

Proposed Rules

For the reasons set forth, the Federal Communications Commission proposes to amend parts 1, 2, and 15 of Title 47 of the Code of Federal Regulations as follows:

PART 1 – PRACTICE AND PROCEDURE

1. The authority citation for part 1 continues to read as follows:

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. 2461 note; 47 U.S.C. 1754, unless otherwise noted.

2. Delayed indefinitely, amend § 1.70006 by revising paragraph (d) to read as follows:

§ 1.70006 Certifications.

* * * * *

(d) That the submarine cable system will not use equipment or services that are produced or provided by an entity identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601-1609 or other covered communications equipment or services wherein the specific determination concerning such equipment or services specifically references national security threats involving submarine cable systems.

3. Delayed indefinitely, amend § 1.70007 by revising paragraph (u) to read as follows:

§ 1.70007 Routine conditions.

* * * * *

(u) No licensee shall add to its submarine cable system(s) under its respective license(s) equipment or services that are produced or provided by an entity identified on the Covered List that the Commission maintains on its website pursuant to the Secure Networks Act, 47 U.S.C. 1601-1609; except, this part of paragraph (u) shall not apply to a licensee that is identified on the Covered List whose cable landing license was or is granted prior to November 26, 2025.

(1) A licensee whose application for a cable landing license is filed and granted after November 26, 2025, shall not use equipment or services that are produced or provided by an entity identified on the Covered List on its submarine cable system under the license.

(i) A licensee whose modification application to add a new segment is filed and granted after November 26, 2025, shall not use equipment or services that are produced or provided by an entity identified on the Covered List on the new segment and the new landing point.

(ii) * * *

* * * * *

Part 2 — FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

4. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336 unless otherwise noted.

5. Amend § 2.803 by changing the title, revising paragraph (c), and redesignating paragraphs (c) and (d) as paragraphs (d) and (e) to read as follows:

§ 2.803 Marketing of radiofrequency devices that lack an equipment authorization

* * * * *

(d) * * *

(3) Notwithstanding paragraph (b), for devices that lack an equipment authorization and are listed on the Covered List, as established pursuant to § 1.50002 of this chapter, marketing is prohibited.

* * * * *

6. Amend part 2 subpart I by adding § 2.804, to read as follows:

§ 2.804 Online Marketing of radiofrequency devices subject to an equipment authorization

(a) Prohibited marketing representations. Online marketplaces shall not market a radiofrequency device subject to equipment authorization in a manner that:

(1) Promotes or encourages operation of the device in violation of the Communications Act or the Commission's rules;

(2) Promotes or encourages modification of the device to operate outside the parameters authorized by the Commission; or

(3) Represents that the device may be used to evade, interfere with, disable, or circumvent lawful communications, regulatory requirements, or technical safeguards.

(b) Required warning for licensed-use devices. Online marketplaces marketing a device subject to authorization shall prominently display the following notice at the online point of sale:

"This equipment may only be sold to end users in the United States who hold the appropriate FCC license. Information regarding the purchase may be provided to the FCC upon request."

(c) Online marketplace obligations. Online marketplaces shall:

(1) Collect the Supplier's Declaration of Conformity compliance information statement or equivalent compliance documentation;

(2) Take reasonable steps to verify that the device is authorized or exempt from authorization under Commission rules;

(3) Maintain such records for a period specified by the Commission; and

(4) Display equipment authorization or compliance information in at the online point of sale.

7. Amend § 2.902 by adding the following definitions, in alphabetical order, to read as follows:

§ 2.902 Terms and definitions.

Covered List sector.

A category of equipment, the entirety of which or a subset of which is listed on the Covered List in § 1.50002 of this chapter.

Hardware bill of materials (HBOM).

A formal record identifying the hardware components contained in a device and information regarding the origin and production of those components.

* * *

Personal use.

Use of a device:

(1) In a manner not intended for sale, lease, marketing, distribution, or other commercial advantage; and

(2) Solely by an individual or a not-for-profit entity for noncommercial purposes.

Produced in a foreign country.

A device is produced in a foreign country if it either:

(1) does not qualify as a domestic end product as that term is defined in 48 CFR § 25.101(a); and

(2) is designed or developed in a foreign country.

* * *

Software bill of materials (SBOM).

A formal record containing details and supply chain relationships of software and firmware components used in a device.

8. Amend § 2.906 by revising subparagraph (d) and adding subparagraphs (e) and (f) to read as follows:

§ 2.906 Supplier's Declaration of Conformity.

(d) Notwithstanding other parts of this section, equipment otherwise subject to the Supplier's Declaration of Conformity process that is produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, or a device within a Covered List sector are prohibited from obtaining equipment authorization through that process. The rules in this chapter governing certification apply to authorization of such equipment.

(e) Registration requirement. Devices authorized pursuant to the Supplier’s Declaration of Conformity process shall be registered with the Commission prior to marketing.

(1) The Commission shall assign a unique identification number for each registered device.

(2) The responsible party shall provide information specified by the Commission, including compliance information, responsible party identification, and device identification information.

(3) Registration information shall be publicly available unless entitled to confidential treatment under § 0.459.

(f) Public Display Requirement. The unique registration identifier shall be displayed:

(1) On the device or its packaging;

(2) In the compliance information statement; and

(3) In online marketing and product listings.

9. Amend § 2.907 by revising subparagraph (c) to read as follows:

§ 2.907 Certification.

* * * * *

(c) Any equipment otherwise eligible for authorization pursuant to the Supplier's Declaration of Conformity, or exempt from equipment authorization, produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, or devices within a Covered List sector must obtain equipment authorization through the certification process. Devices subject to this paragraph shall comply with all certification application requirements set forth in this subpart, including disclosure and reporting obligations applicable to certification applicants.

* * * * *

10. Amend § 2.909 to read as follows:

§ 2.909 Responsible Party and Liable Party

(a) Responsible Party.

(1) In the case of equipment that requires the issuance of a grant of certification, the party to whom that grant of certification is issued is responsible for the compliance of the equipment with the applicable technical and other requirements. If any party other than the grantee modifies the radio frequency equipment and that party is not working under the authorization of the grantee pursuant to § 2.929(b), the party performing the modification is responsible for compliance of the product with the appliable administrative and technical provisions in this chapter.

(2) For equipment subject to Supplier's Declaration of Conformity the party responsible for the compliance of the equipment with the applicable standards, who must be located in the United States (see § 2.1077), is set forth as follows:

(A) The manufacturer or, if the equipment is assembled from individual component parts and the resulting system is subject to authorization under Supplier's Declaration of Conformity, the assembler.

(B) If the equipment by itself, or, a system is assembled from individual parts and the resulting system is subject to Supplier's Declaration of Conformity and that equipment or system is imported, the importer.

(C) Retailers or original equipment manufacturers may enter into an agreement with the responsible party designated in paragraph (b)(1) or (b)(2) of this section to assume the responsibilities to ensure compliance of equipment and become the new responsible party.

(D) If the radio frequency equipment is modified by any party not working under the authority of the responsible party, the party performing the modifications, if located within the U.S., or the importer, if the equipment is imported subsequent to the modifications, becomes the new responsible party.

(3) If the end product or equipment is subject to both certification and Supplier's Declaration of Conformity (i.e., composite system), all the requirements of paragraphs (a) and (b) of this section apply.

(4) If, because of modifications performed subsequent to authorization, a new party becomes responsible for ensuring that a product complies with the technical standards and the new party

does not obtain a new equipment authorization, the equipment shall be labeled, following the specifications in § 2.925(d), with the following: "This product has been modified by [insert name, address and telephone number or internet contact information of the party performing the modifications].

(5) In the case of transfer of control of equipment, as in the case of sale or merger of the responsible party, the new entity shall bear the responsibility of continued compliance of the equipment.(b) Liable Party. In the case that the grantee of equipment authorization through certification is located in a foreign country, there must be a liable party located in the United States. The party liable for compliance of the equipment with the applicable standard and Commission rules is set forth as follows:

(1) The manufacturer or, if the equipment is assembled from individual component parts and the resulting system is subject to authorization under certification, the assembler.

(2) If the equipment by itself, or, a system is assembled from individual parts and the resulting system is subject to certification and that equipment or system is imported, the importer.

(3) Retailers or original equipment manufacturers may enter into an agreement with the liable party designated in paragraph (b)(1) or (b)(2) of this section become the new liable party.

(4) If the radio frequency equipment is modified by any party not working under the authority of the responsible party, the party performing the modifications, if located within the U.S., or the importer, if the equipment is imported subsequent to the modifications, becomes the new liable party.

11. Amend § 2.911(d) by adding subparagraphs (8) to (11) to read as follows:

§ 2.911 Application requirements.

* * * * *

(8) The applicant shall provide a written and signed certification identifying any and all entities that produced the device for which equipment authorization is sought.

(i) The certification shall identify each entity that produced the device, including any entity involved in the design, development, manufacturing, or assembly of the device.

(ii) The certification shall be signed by an authorized representative of the applicant.

(iii) The applicant shall update the certification if material changes occur prior to grant of the equipment authorization.

(iv) The Commission or Telecommunication Certification Body may request additional information reasonably necessary to determine whether an identified entity produced the device.

(9) Supply chain disclosure materials.

(i) An applicant for certification shall submit, as part of its application, a written and signed hardware bill of materials (HBOM) and software bill of materials (SBOM) for the device for which equipment authorization is sought.

(ii) The HBOM and SBOM shall identify all components of the device, including hardware, software, and firmware components of the device.

(iii) The HBOM and SBOM shall be certified as true and correct by an authorized representative of the applicant.

(iv) The Commission or Telecommunication Certification Body may require the applicant to provide supplemental documentation sufficient to verify the accuracy or completeness of the

HBOM or SBOM.

(10) Required contents of HBOM and SBOM disclosures. The HBOM and SBOM required by paragraph (d)(9) of this section shall identify, for each critical component:

(i) The component name and function;

(ii) The producer of the component;

(iii) The location or locations where the component was designed, developed, manufactured, assembled, or otherwise produced;

(iv) The percentage of component value attributable to each producer and production location; and

(11) Producer contact information. For each producer identified pursuant to this section or within any required HBOM or SBOM submission, the applicant shall provide:

(i) The producer's legal name;

(ii) Any trade names or doing-business-as names used by the producer;

(iii) The producer's principal place of business;

(iv) The jurisdiction of incorporation or organization;

(v) Contact information for an authorized representative of the producer, including mailing address, telephone number, and electronic mail address; and

(vi) Any additional identifying or contact information required by the Commission or Telecommunication Certification Body for purposes of verifying production location or supply chain information.

12. Amend 2.931 to add subparagraph (g) to read as follows:

§ 2.931 Responsibilities

* * * * *

(f) The responsible party shall update any HBOM or SBOM information submitted pursuant to § 2.911 within 30 days of any material change to the hardware, software, firmware, producer, or production location information contained therein.

* * * * *

13. Revise § 2.932(b) to add a final sentence to subparagraph (b) to read as follows:

§ 2.932 Modification of equipment.

* * * * *

(b) * * * Notwithstanding this section, software or firmware updates to already-authorized covered equipment shall not constitute a request for a new equipment authorization where:

(1) The modification mitigates harm to consumers

(2) The modification does not enhance the device's capability or alter its intended use;

(3) The modified device is marketed as an identical; and

(4) product to the pre-modified device

* * * * *

14. Amend § 2.939 by deleting paragraph (b), redesignating paragraph (c) as paragraph (b), adding a paragraph (c), and amending paragraph (d) to read as follows:

§ 2.939 Revocation, withdrawal, or limitation of equipment authorization.

(b) [Remove]

(b) The Commission may withdraw an equipment authorization in the event of changes in its technical standards. The procedure to be followed will be set forth in the order promulgating such new technical standards (after appropriate rulemaking proceedings) and will provide a suitable amortization period for equipment in hands of users and in the manufacturing process.

* * * * *

(c) Notwithstanding other provisions of § 2.939, the Commission directs the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to revoke equipment authorizations using the streamlined process in paragraph (d) for any of the following equipment authorizations:

(1) any case of willfulness, such as false statements or misrepresentations to the Commission, by a test lab, a TCB, or another federal agency, involving an equipment authorization application or existing grant;

(2) any willful failure to provide required information associated with the equipment authorization to the Commission, a test lab, a TCB, or another authorized federal agency;

(3) any equipment authorization for equipment that has been granted a Conditional Approval, but which Conditional Approval has been subsequently terminated.

(d) The streamlined revocation process shall be:

(1) If the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau determine that one of the conditions in paragraph (c) is met, they will provide written notice to the grantee that a revocation proceeding is being initiated and the grounds under consideration for such revocation.

(2) The grantee will have 10 days in which to respond in writing to the reasons cited for initiating the revocation proceeding. The Office of Engineering and Technology and the Public Safety and Homeland Security Bureau will then review the submissions, request additional information as may be appropriate, and make their determination as to whether to revoke the authorization, providing the reasons for such decision.

* * * * *

15. Amend § 2.1043 by adding paragraph (m) to read as follows:

§ 2.1043 Changes in certificated equipment.

* * * * *

(m) Software, firmware, or hardware updates to already-authorized covered equipment shall constitute Class I or Class II permissive changes respectively, shall not constitute applications for equipment authorizations, and are not be prohibited, so long as:

(1) The modification mitigates harm to consumers;

(2) The modification does not enhance the device's capability or alter its intended use;

(3) The modified device is marketed as an identical product to the pre-modified device; and

(4) involve swapping a U.S.-made component for a non-U.S. made component.

16. Amend § 2.1074 by adding subparagraphs (c) and (d) to read as follows:

* * * * *

(c) The FCC logo shall not be affixed to, displayed on, or associated with incidental radiators or any other devices not subject to equipment authorization requirements under this chapter.

(d) The FCC logo shall not be used on, displayed in connection with, or associated with any device that:

(1) Has not been properly tested and authorized in accordance with the Commission's rules;

(2) Is marketed in violation of the Commission's equipment authorization requirements;

(3) Has had its equipment authorization revoked, withdrawn, suspended, or limited; or

(4) Is otherwise not eligible to bear the FCC logo under this chapter.

* * * * * *

17. Amend § 2.1204, by removing the last word from subparagraph (a)(5), removing subparagraphs (a)(5)(i) and (ii), and adding subparagraph (c), to read as follows:

§ 2.1204 Import conditions.

(a) * * *

* * * * *

(5) The radio frequency device is being imported solely for export. The device will not be marketed or offered for sale in the U.S.

* * * * *

(c) Covered equipment. Notwithstanding paragraph (a) of this section, covered equipment may be imported only if one or more of the following conditions are satisfied:

(1) The equipment has a valid equipment authorization that has not been limited, revoked, or otherwise restricted pursuant to § 2.939(e);

(2) The equipment is imported in a quantity of 40 or fewer units for testing and evaluation or product development, unless the Chief of the Office of Engineering and Technology grants written approval for a greater quantity;

(3) The equipment is imported solely for export;

(4) The equipment is imported exclusively for use by the United States Government; or

(5) The equipment is imported solely for the purpose of developing products for use exclusively by the United States Government.

PART 15 – RADIO FREQUENCY DEVICES

18. The authority citation for part 15 continues to read as follows:

Authority: 47 U.S.C. 154, 302A, 303, 304, 307, 336, 544A and 549.

19. Amend § 15.101 by adding subparagraph (f), to read as follows:

§ 15.101 Equipment authorization of unintentional radiators.

* * * * *

(f) Notwithstanding any other provision of this section, devices within a Covered List sector shall be subject to certification.

APPENDIX C

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) incorporated an Initial Regulatory Flexibility Analysis (IRFA) in the *Second Equipment Authorization Security Report and Order, Order, and Further Notice of Proposed Rulemaking* (*Second Report and Order and Second Further Notice*).[2] The Commission sought written public comment on the proposals in the *Second Report and Order and Second Further Notice*, including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA and it (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Rules

2. In the *Second Report and Order and Second Further Notice*, the Commission expanded upon previously adopted rules to further proscribe the authorization of communications equipment determined to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons" under our equipment authorization program (EA program).[4] Such equipment, also known as "covered equipment," is identified on the Commission's Covered List.[5] In the *Third Report and Order*, the Commission takes additional action to strengthen the Commission's equipment authorization (EA) program against national security risks to the communications supply chain by adopting clarifications and revisions to our part 2 rules.[6] Specifically, we close previous loopholes by prohibiting the authorization of devices that include logic-bearing hardware components that are covered equipment. We further require that any modification or permissive changes by entities identified on the Covered List undergo full certification and clarify that the marketing rules reach any entity—including e-commerce platforms—that market unauthorized equipment. Finally, we require online marketplaces to provide an FCC ID at the online point of sale. The adoption of these rule clarifications and revisions will further our goals of strengthening the security of the Commission's EA program and, by extension, our national security.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

3. No comments were filed addressing the impact of the proposed rules on small entities.

C. Response to Comments by the Chief Counsel for the Small Business Administration

[1] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[2] *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 (2025) (*Second Report and Order and Second Further Notice*).

[3] 5 U.S.C. § 604.

[4] *See Second Report and Order and Second Further Notice*.

[5] Pursuant to sections 2(a) and (d) of the Secure and Trusted Communications Networks Act of 2019, and sections 1.50002 and 1.50003 of the Commission's rules, the Federal Communications Commission's Public Safety and Homeland Security Bureau (PSHSB) publishes a list of communications equipment and services that have been determined by one of the sources specified in that statute to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons (covered equipment). Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609 (Secure Networks Act); 47 CFR §§ 1.50002, 1.50003.

[6] *See supra, at para.* 13.

Office of Advocacy

4. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA,[7] the Commission is required to respond to any comments filed by the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy, and also provide a detailed statement of any change made to the proposed rules as a result of those comments.[8] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

5. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the adopted rules.[9] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[10] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[11] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[12] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[13]

Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions.[14]

6. In general, a small business is an independent business having fewer than 500 employees.[15] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[16] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and are not dominant in their field.[17] While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees.[18] Finally, "small governmental jurisdictions" are defined as cities, counties, towns,

---

[7] Small Business Jobs Act of 2010, Pub. L. No. 111-240, 124 Stat. 2504 (2010).

[8] 5 U.S.C. § 604 (a)(3).

[9] *Id*. § 604.

[10] *Id*. § 601(6).

[11] *Id*. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[12] 15 U.S.C. § 632.

[13] 13 CFR 121.903.

[14] 5 U.S.C. § 601(3)-(6).

[15] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[16] *Id*.

[17] 5 U.S.C. § 601(4).

[18] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

townships, villages, school districts, or special districts with populations of less than fifty thousand.[19] Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.[20]

7. The rules adopted in the *Third Report and Order* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[21] codes and corresponding SBA size standard.[22] Where available, we also provide additional information regarding the number of potentially affected entities in the identified industries below.

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	**NAICS Code**	**SBA Size Standard**	**Total Firms[23]**	**Total Small Firms[24]**	**% Small Firms**
Electronic Computer Manufacturing	334111	1,250 employees	148	128	86.49%
Computer Terminal Manufacturing	334118	1,000 employees	201	194	96.52%
Telephone Apparatus Manufacturing[25]	334210	1,250 employees	155	136	87.74%
Radio and Television Broadcasting and Wireless Communications Equip	334220	1,250 employees	155	136	87.74%

[19] 5 U.S.C. § 601(5).

[20] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

[21] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

[22] The size standards in this chart are set forth in 13 CFR 121.201, by six digit NAICS code.

[23] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[24] *Id.*

[25] Affected Entities in this industry include Multi-Line Telephone System Manufacturers Importers Sellers or Lessors.

Manufacturing[26]					
Other Communications Equipment Manufacturing[27]	334290	800 employees	310	294	94.84%
Audio and Video Equipment Manufacturing	334310	750 employees	506	492	97.23%
Semiconductor and Related Device Manufacturing	334413	1,250 employees	675	610	90.37%
Search Detection Navigation Guidance...Nautical Sys and Instrument Manufacturing	334511	1,350 employees	404	369	91.34%
Aircraft Manufacturing[28]	336411	1,500 employees	234	209	89.32%
Medical Laboratories	621511	$41.5 million	4,527	3,525	77.87%
Uncrewed Aircraft System (UAS) Operators	None	100 employees or less[29]	Data Not Disclosed	Data Not Disclosed	92.20%[30]

E. Description of Economic Impact and Projected Reporting, Recordkeeping and Other Compliance Requirements for Small Entities

8. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.[31]

9. In the *Third Report and Order*, we build upon the steps taken in the *Second Report and Order and Second Further Notice*, by amending the Commission's part 2 rules concerning the equipment authorization program's requirements, processes, and guidance to include additional provisions and further clarification of our current reporting and certification requirements. Specifically, the adopted rules affect small entity grantees that seek authorization of any equipment identified on the Covered List that fails to comply with our rules regarding covered equipment. Further, the adopted rules address the prohibited authorization of devices that contain logic-bearing hardware components produced by entities

[26] Affected Entities in this industry include Aviation Radio Equipment Manufacturers, Broadcast Auxiliary Services (BAS) Remote Pickup (RPU) Manufacturing, Part 15 Handset Manufacturers, Radio Frequency Equipment Manufacturers, Uncrewed Aircraft Radio Equipment Manufacturers, Vendors of Infrastructure Development_Network Buildout.

[27] Affected Entities in this industry include Radio Frequency Equipment Manufacturers (Non-standard specialized equipment) and Vendors of Infrastructure Development_Network Buildout.

[28] Affected Entities in this industry include Uncrewed Aircraft Radio Equipment Manufacturers.

[29] *See* Federal Aviation Administration, Department of Transportation, Remote Identification of Unmanned Aircraft, 86 Fed. Reg. 4390, 4494 (Jan. 15, 2021) (*Remote ID Rule*).

[30] *Id.*

[31] 5 U.S.C. § 604(a)(5).

identified on the Covered List, prohibition on importation and marketing, and those posing unacceptable risks to national security. The adopted rules also affect online marketplaces that must display FCC IDs for certified equipment at the online point of sale. The Commission expects that all filing, recordkeeping, and reporting requirements associated with the adopted rules will be the same for small and other entities. Moreover, the existing record does not reflect that the rules adopted today would disproportionately affect small entities.

10. The Commission expects that the actions taken in the *Third Report and Order* will efficiently advance our nation's security objectives without incurring substantial costs to small and other entities. For example, some measures, such as the prohibition of logic-bearing hardware components and the broad scope of the prohibition on authorization of equipment identified on the covered list, are simply minimal changes reflecting clarifications of measures previously taken and, as such, should present minimal compliance costs to small entities. Broad alternatives—such as banning all components produced by any foreign -adversary -controlled actor—were rejected because they would impose sweeping and disproportionate burdens on small entities. Other measures, such as the requirement to display FCC IDs for certified equipment at the online point of sale, are also minimal changes; online marketplaces already post comprehensive product information, and adding a single identifier does not increase marginal effort or expense. In addition, while we cannot conclusively determine whether the rules adopted in the *Third Report and Order* will necessitate the need for small entities to hire professionals to assist them with complying with the adopted rules, we note that the comments in the existing record do not indicate such a need.

11. With the adoption of the *Third Report and Order*, the further revisions to the rules will help advance the Commission's goals of protecting national security and public safety from threats to the communications supply chain and help to ensure we have the necessary information to prohibit authorization of equipment deemed to be a threat to our nation's communications systems.

F. Discussion of Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

12. The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities…including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[32]

13. The *Third Report and Order* adopts revisions to the Commission's part 2 rules regarding covered equipment identified on the Covered List in order to protect our nation's communications systems from equipment that poses a national security risk or a threat to the safety of U.S. persons. Future prohibitions of covered equipment are mandated by the Secure Equipment Act, requiring that the Commission prohibit existing covered equipment, authorization or approval of any application for covered equipment, such as logic-bearing hardware components in devices. Pursuant to Executive Order 12866, the Commission considered alternatives to this rule that would impose less of a societal burden. We did not find any reasonable alternative that would have decreased the impact on small entities but still achieve the objective of the rule.

14. Through its review of the record in this proceeding and in its ultimate adoption of the rules set forth in the *Third Report and Order*, the Commission has sought, where practicable, to minimize significant economic impact to small entities and, in doing so, has considered significant alternatives to those adopted today. For example, the adopted rules have been narrowly tailored to account for commenter concerns that an overly broad approach to limiting previously granted authorizations of covered equipment would create significant financial and technological burdens to small and other entities that may lack the financial or human resources to effectively comply with the new rules. In

[32] *Id*. § 604(a)(6).

addition, we also considered preserving the status quo by not adopting any new measures to address the persistent vulnerabilities identified in the record. While this alternative would, on the surface, provide the least amount of immediate regulatory cost impact, it would carry substantial hidden costs in the form of heightened exposure to national security threats. In making our determinations in this proceeding, we believe that the costs we are imposing are reasonable in light of our national security goals.

G. Report to Congress

15. The Commission will send a copy of the *Third Report and Order*, including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act.[33] In addition, the Commission will send a copy of the *Third Report and Order*, including this Final Regulatory Flexibility Analysis, to the Chief Counsel for the SBA Office of Advocacy and will publish a copy of the *Third Report and Order*, and this Final Regulatory Flexibility Analysis (or summaries thereof) in the Federal Register.[34]

[33] 5 U.S.C. § 801(a)(1)(A).

[34] *Id.* § 604(b).

APPENDIX D

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *Third Further Notice of Proposed Rulemaking* (*Third Further Notice*) assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *Third Further Notice*. The Commission will send a copy of the *Third Further Notice*, including this IRFA, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.[2] In addition, the *Third Further Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

2. In the *Second Report and Order and Second Further Notice*, the Commission sought comment on how best to strengthen our prohibitions regarding the authorization of covered equipment and to clarify and enforce its related rules. In the *Third Further Notice*, the Commission proposes and seeks comment on additional measures to close loopholes, strengthen supply-chain visibility, and modernize enforcement mechanisms. These measures include: Bifurcating Covered List rules into producer/provider-based and production-location-based categories; further prohibition on authorization of devices containing any component or associated element, including software, by a foreign adversary or Covered List entity; requiring hardware bills of material (HBOM) and software bills of material SBOM) submission for new authorizations; requiring registration for all SDoC devices; updating definitions relating to the Covered List ("produced by," "critical infrastructure," "produced in a foreign country"); strengthening rules governing white labeling, electrically identical devices, and modular-transmitter loopholes; modernizing importation, marketing, and pre-authorization operation rules; considering term limits for equipment authorizations; and expanding enforcement tools, including streamlined revocation procedures. Through these proposals, the Commission aims to prevent exploitation of gaps in the equipment authorization (EA) process while enabling future technological innovation.

B. Legal Basis

3. The proposed action is authorized pursuant to sections 4(i), 301, 302, 303, 403, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 301, 302a, 303, 403, 503, and the Secure Equipment Act of 2021, Pub. L. 117-55, 135 Stat. 423.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[4] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[5] In addition, the term "small business" has the

[1] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[2] *Id.* § 603(a).

[3] *Id*.

[4] 5 U.S.C. § 603(b)(3).

[5] *Id*. § 601(6).

same meaning as the term "small business concern" under the Small Business Act.[6] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[7] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[8]

5. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions.[9] In general, a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[11] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant in their field.[12] While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees.[13] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[14] Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.[15]

6. The rules proposed in the *Third Further Notice* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[16] codes and corresponding SBA size standard.[17] Where available, we also provide additional information regarding the number of potentially affected entities in the industries identified below.

Regulated Industry	NAICS Code	SBA Size	Total	Total Small	% Small Firms

[6] *Id*. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[7] 15 U.S.C. § 632.

[8] 13 CFR 121.903.

[9] 5 U.S.C. § 601(3)-(6).

[10] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[11] *Id*.

[12] 5 U.S.C. § 601(4).

[13] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

[14] 5 U.S.C. § 601(5).

[15] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

[16] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

[17] The size standards in this chart are set forth in 13 CFR 121.201, by six digit North American Industrial Classification System (NAICS) code.

(Footnotes specify potentially affected entities within a regulated industry where applicable)		Standard	Firms[18]	Firms[19]	
Electronic Computer Manufacturing	334111	1,250 employees	148	128	86.49%
Computer Terminal Manufacturing	334118	1,000 employees	201	194	96.52%
Telephone Apparatus Manufacturing[20]	334210	1,250 employees	155	136	87.74%
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing[21]	334220	1,250 employees	155	136	87.74%
Other Communications Equipment Manufacturing[22]	334290	800 employees	310	294	94.84%
Audio and Video Equipment Manufacturing	334310	750 employees	506	492	97.23%
Semiconductor and Related Device Manufacturing	334413	1,250 employees	675	610	90.37%
Search Detection Navigation Guidance...Nautical Sys and Instrument Manufacturing	334511	1,350 employees	404	369	91.34%

[18] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[19] *Id.*

[20] Affected Entities in this industry include Multi-Line Telephone System Manufacturers Importers Sellers or Lessors.

[21] Affected Entities in this industry include Aviation Radio Equipment Manufacturers, Broadcast Auxiliary Services (BAS) Remote Pickup (RPU) Manufacturing, Part 15 Handset Manufacturers, Radio Frequency Equipment Manufacturers, Uncrewed Aircraft Radio Equipment Manufacturers, Vendors of Infrastructure Development_Network Buildout.

[22] Affected Entities in this industry include Radio Frequency Equipment Manufacturers (Non-standard specialized equipment) and Vendors of Infrastructure Development_Network Buildout.

Aircraft Manufacturing[23]	336411	1,500 employees	234	209	89.32%
Medical Laboratories	621511	$41.5 million	4,527	3,525	77.87%
Uncrewed Aircraft System (UAS) Operators	None	100 employees or less[24]	Data Not Disclosed	Data Not Disclosed	92.20%[25]

D. Description of Economic Impact and Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

7. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record. [26]

8. In the *Third Further Notice*, the Commission seeks comment on ways in which we could strengthen our prohibitions on the authorization of covered equipment and how best to clarify the rules and enforcement of such proposals. If adopted, additional or revised rules resulting from the inquiries made in the *Third Further Notice* may create additional reporting, recordkeeping, and other compliance requirements for small entities. For example, the proposals in the *Third Further Notice* could introduce new compliance responsibilities, such as software bill of materials (SBOM) and hardware bill of material (HBOM) filings with updates after material changes, Suppliers' Declaration of Conformity (SDoC) device registration with unique identifiers, expanded certification disclosures, including identification of all producers, possible term-limited authorization renewal filings, and enhanced importation documentation for Covered List equipment.

9. The Commission also seeks comment from small entities and other interested parties to assist us with the clarification of specific terms and in determining how covered equipment is identified. We will developing our assessment of the economic impact of reporting, recordkeeping, or other compliance requirements on small entities as additional information is added to the record. In addition, while we do not anticipate that small entities would need to hire professionals to comply with any rules that are ultimately adopted as a result of the responses to our inquiries herein, we seek comments from small entities specific to any potential economic or regulatory burdens or costs that would assist the Commission with promulgating future regulations that may establish new requirements for small entities.

E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

10. The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities.[27] The discussion is required to include alternatives such as: "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance

[23] Affected Entities in this industry include Uncrewed Aircraft Radio Equipment Manufacturers.

[24] *See* Federal Aviation Administration, Department of Transportation, Remote Identification of Unmanned Aircraft, 86 Fed. Reg. 4390, 4494 (Jan. 15, 2021) (*Remote ID Rule*).

[25] *Id.*

[26] 5 U.S.C. § 603(b)(4).

[27] *Id.* § 603(c).

rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[28]

11. As discussed above, the *Second Report and Order* and *Second Further Notice* sought comment on how best to strengthen our prohibitions regarding the authorization of covered equipment and the clarification and enforcement of its related rules. However, those rules do not fully address the Commission's statutory responsibilities, thus necessitating the *Third Further Notice's* request for additional comment. In formulating its request for comments in the *Third Further Notice*, the Commission considered alternatives addressing the economic impact of its proposals on small entities, should they be adopted. We considered maintaining the status quo, however doing so would be rejecting increased security controls. We also considered adopting a blanket ban on all foreign-produced components, however we rejected such an approach as overly burdensome. By seeking additional comment and considering other approaches, the Commission could clarify the scope of activities that constitute the authorization prohibitions, the marketing of equipment and measures to strengthen the enforcement of marketing prohibitions. We also note that in developing our proposed rules, we have designed them to be narrowly tailored to specific, well-supported national security determinations, thereby ensuring that the Commission strengthens protections while avoiding unnecessary disruption to lawful supply chains.

12. The Commission will fully consider the economic impact on small entities as it evaluates the comments filed in response to the *Third Further Notice*, including comments related to costs and benefits. Alternative proposals and approaches from commenters would further develop the record and could help the Commission further minimize the economic impact on small entities. The Commission's evaluation of the comments filed in this proceeding would shape the final conclusions it reaches, the final alternatives it considers, and the actions it ultimately takes to minimize any significant economic impact that may occur on small entities from the final rules.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

13. None.

[28] *Id.* § 603(c)(1)-(4).