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
	)	
	)	
	)	

SECOND REPORT AND ORDER AND SECOND FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: October 28, 2025 **Released: October 29, 2025**

By the Commission: Chairman Carr and Commissioner Trusty issuing separate statements.

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]

TABLE OF CONTENTS

I. INTRODUCTION

1. In November 2022, as part of the Federal Communications Commission's (FCC or Commission) ongoing efforts to protect the security of America's communications networks and equipment supply chains, the Commission adopted the *Equipment Authorization Security Report and Order, Order, and Further Notice of Proposed Rulemaking* (*EA Security R&O and FNPRM*).[1] In that item, the Commission adopted rules as part of its equipment authorization program to prohibit authorization of communications equipment that has been determined to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons" (covered equipment), which the Commission publishes in its Covered List.[2] The rules constituted significant changes to the prior equipment authorization program. The Commission recognized that these revisions were only first steps and that further revisions should be considered to better ensure effective implementation of this prohibition. In the FNPRM portion of the item, the Commission sought comment on taking additional steps in our equipment authorization program to protect our nation's communications networks and supply chains. Building on the record received, our experience implementing the prohibition, and other recent Commission actions aimed at protecting our nation's communications networks and supply chain, we adopt this Second Report and Order (Second R&O) and Second Further Notice of Proposed Rulemaking (Second FNPRM) to take important next steps in modifying our equipment authorization program.

2. *Executive summary.* In the Second R&O, we provide further guidance on the prohibition on authorization of covered equipment, prohibit the authorization of devices that contain certain component parts identified on the Covered List, adopt a procedure to implement prohibitions on the continued importation and marketing[3] of previously authorized covered equipment–without affecting continued operation or use, and clarify when equipment is deemed to be "produced by" a particular entity for purposes of these rules. In the Second FNPRM, we seek further comment on issues related to modules and component parts in terms of the Covered List, propose definitions for "critical infrastructure" in terms of the Covered List, propose modification to our permissive change procedures with regard to covered equipment, discuss clarifications to the definitions of "importation" and "marketing" as used in part 2 of our rules, and propose measures to strengthen enforcement against unauthorized marketing.

3. We summarize the Second R&O and Second FNPRM as follows:

- Second R&O:

---

[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) (*EA Security R&O and FNPRM*). The instant Second R&O and Second FNPRM only addresses issues in ET Docket No. 21-232 concerning matters relating to the Commission's equipment authorization program and does not address matters relating to the Commission's competitive bidding program raised in EA Docket No. 21-233.

[2] 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. For the current version of the Covered List, *see* Federal Communications Commission, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist (last updated July 23, 2025).

[3] "Marketing" as used here "includes 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." 47 CFR § 2.803(a).

  - Clarifies that, for purposes of the Covered List, covered equipment includes modular transmitters, so modular transmitters are prohibited from individual authorization.
  - Prohibits authorization of devices that include modular transmitters that are covered equipment.
  - Provides a procedure to limit previously granted authorizations of covered equipment to prohibit the continued importation and marketing of such equipment, without limiting continued operation or use.
  - Clarifies the term "produced by" as used in our rules and some existing Covered List entries.
  - Clarifies the prohibition on modification, including permissive changes, to previously authorized covered equipment or equipment that would become covered as a result of such modification or permissive change.
- Second FNPRM:
  - Seeks additional comment on modular transmitters and component parts in relation to covered equipment.
  - Proposes a definition of "critical infrastructure" as used on the Covered List and seeks comment on the implementation of that definition.
  - Seeks comment on whether any device modification made by an entity identified on the Covered List should require full certification.
  - Seeks comment on clarifying the scope of activities that constitute marketing of equipment.
  - Seeks comment on measures to strengthen enforcement of marketing prohibitions.

4. The clarifications and rule revisions we adopt in this Second Report and Order and the additional information we seek through the Second FNPRM are aimed at furthering our goals of continuing to strengthen the security of our equipment authorization program.

II. BACKGROUND

5. Enacted in March 2020, the Secure Networks Act requires the Commission to publish a list of equipment and services that pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons" based solely on specific determinations made by certain enumerated sources (Covered List).[4] In June 2021, the Commission initiated this proceeding in its *Equipment Authorization Security Notice of Proposed Rulemaking* (*EA Security NPRM*), ET Docket No. 21-232.[5] The Commission noted that this proceeding – which involves revising the Commission's equipment authorization program – is part of the Commission's overall efforts in carrying out its important role in protecting the security of America's equipment supply chains, and also is part of the ongoing efforts of Congress, the Executive Branch, and the Commission to identify and eliminate potential security vulnerabilities in communications networks and supply chains.[6]

[4] Secure Networks Act, § 2(b)-(c). There is one narrow exception to this exclusivity. *See* National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-234, § 1709(a)(2) (2024) (2025 NDAA) (directing the Commission to add certain communications equipment and services related to Unmanned Aircraft Systems to the Covered List in the event that no appropriate national security agency makes a specific determination within one year of enactment, *i.e.* December 23, 2025).

[5] *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 & EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd 10578 (2021) (*EA Security NPRM*).

[6] *EA Security NPRM*, 36 FCC Rcd at 10580-89, paras. 1, 5-22.

6. In the *EA Security R&O and FNPRM*, the Commission established several new rules to prohibit authorization of equipment identified on the Commission's Covered List developed pursuant to the Secure Networks Act.[7] In particular, the Commission adopted several revisions to our part 2 rules concerning equipment authorization requirements, processes, and guidance that involve significant changes to the equipment authorization program. These changes include new requirements placed on applicants seeking equipment authorizations as well as "responsible parties" associated with equipment authorizations and entities that are identified on the Covered List. These rules also place significant new responsibilities on telecommunication certification bodies (TCBs), private third-party organizations recognized by the Commission and to which the Commission has delegated particular responsibilities pursuant to section 302 of the Act.[8] TCBs are now tasked with reviewing equipment authorization applications and certifying that the subject equipment complies with all applicable Commission requirements, both technical (such as based on information submitted by test labs) and non-technical (such as those prohibiting authorization of covered equipment).[9]

7. These rules require that, going forward, no communications equipment produced by entities identified on the Covered List can obtain an equipment authorization unless the authorization is pursuant to the certification process, which would require filing an application with supporting data that TCBs review. Our rules no longer permit authorization of any such equipment through the Supplier's Declaration of Conformity (SDoC) procedures, which does not require an application filing, nor can such equipment now qualify for any exemption from the need for an equipment authorization.[10] To help implement the prohibition on authorization of any covered equipment, applicants seeking such authorization are required to make certain attestations (in the form of certifications) about the equipment for which they seek authorization–these include attesting that the equipment is not covered and indicating whether the applicant is an entity identified on the Covered List.[11] To further help with implementation of the prohibition, the Commission adopted a requirement that each of the entities named on the Covered List file a report with the Commission identifying its associated but unnamed entities (e.g., its subsidiaries and affiliates).[12] TCBs, pursuant to their responsibilities as part of the Commission's equipment authorization program, review the applications and must ensure that only devices that meet all of the Commission's applicable technical and non-technical requirements are ultimately granted authorization,

---

[7] *See generally EA Security R&O and FNPRM*, 37 FCC Rcd at 13509-98, paras. 32-263. The Commission again explained that this proceeding builds upon the important ongoing efforts by the Commission, Congress, and the Executive Branch to take further action to protect the security of America's critical communications networks and equipment supply chain. *Id.* at 13494-95, para. 1; *see also id.* at 13497-505, 13507-08, paras. 5-23, 31. The Commission found that it had the requisite legal authority to make changes to its equipment authorization program pursuant to the Communications Act of 1934, as amended (the Act), the Secure Networks Act, and the Secure Equipment Act. *Id*. at 13509-13, paras. 32-43.

[8] Section 302(a) of the Act provides that the Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations governing the interference potential of RF devices, and section 302(e) provides that the Commission may authorize the use of private organizations for testing and certifying compliance of RF devices and "establish such qualifications and standards as it deems appropriate for such private organizations, testing, and certification." 47 U.S.C. § 302a(a), (e).

[9] *See, e.g.*, 47 CFR § 2.960(a) (the TCB shall review the application to determine compliance with the Commission's requirements).

[10] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13525-27, 13531-33, paras. 75-79, 97-100.

[11] *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).

[12] The Commission adopted a revision to the subsidiary and affiliate reporting requirement in section 2.903(b) of our rules on May 22, 2025. *EA Integrity R&O*, paras. 87-89. The effective date of that revision is pending review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act.

and that none of these grants are for covered equipment.[13] To help TCBs perform their responsibilities, and to provide guidance to TCBs, applicants, and other interested parties, the Commission provides guidance on what constitutes covered equipment, with delegated authority to the Office of Engineering and Technology (OET) and the Public Safety and Homeland Security Bureau (PSHSB) to update that guidance as appropriate.[14] The Commission has also adopted streamlined revocation procedures for authorizations of equipment in cases in which an applicant submitted false statements or representations in the newly required attestations relating to the equipment for which they had sought authorization.[15]

8. In adopting the *EA Security R&O and FNPRM*, the Commission decided not to require, at that time, that the applicant make attestations that address individual component parts contained within the applicant's equipment[16] and it did not revoke previously granted authorizations of covered equipment.[17] The Commission determined that both of these matters, along with several other issues, would receive further consideration.

9. The Commission sought comment on whether the presence of certain component parts would result in the device being covered equipment prohibited from authorization and, if so, how the prohibition should be implemented in the Commission's equipment authorization program.[18] It also sought comment on the role that applicants and responsible parties would play were the Commission to prohibit authorization of devices that include certain component parts.[19] In addition, it sought comment on the extent to which the Commission should revoke any previous authorizations of covered equipment and, if so, based on which considerations and procedures, and the scope such revocations should take,[20] as well as the extent to which it should take into account supply chain considerations.[21] It also sought comment on whether to require all applicants seeking equipment certification to have a U.S.-based responsible party to help ensure compliance with the Commission's equipment authorization program rules.[22] Finally, the Commission sought comment on various other issues concerning implementation of the prohibition on authorization of covered equipment, such as applicants' provision of additional information on equipment; additional activities that TCBs should conduct in light of the goals of this proceeding; the review of authorizations after grant by TCBs through post-market surveillance; and enforcement of the Commission's newly-adopted rules.[23]

10. *Recent developments concerning the equipment authorization program.* In 2023, Hikvision USA, Inc. and Dahua Technology USA, Inc. petitioned the U.S. Court of Appeals for the District of Columbia Circuit to review aspects of the Commission's *EA Security R&O and FNPRM* that affected them.[24] On April 2, 2024, the court issued a partial remand concerning one part of the Commission's

[13] *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).

[14] *Id.* at 13567-78, paras. 189-215.

[15] *Id.* at 13536-37, paras. 112-13; 47 CFR § 2.939(d).

[16] *Id.* at 13519, para. 57.

[17] *Id.* at 13535, para. 107.

[18] *Id.* at 13602-06, paras. 271-87.

[19] *Id.* at 13605-06, para. 286.

[20] *See Id.* at 13606-12, paras. 288-308.

[21] *Id.* at 13612, paras. 309-310.

[22] *Id.* at 13613-15, paras. 311-318.

[23] *See Id.* at 13615-16, paras. 319-326. We note that while the Commission sought comment on various issues relating to TCBs, it did not seek any specific comment on test labs.

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

decision.[25] Specifically, the court vacated those portions of the Commission's decision defining "critical infrastructure" for purposes of understanding when video surveillance and telecommunications equipment produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), and Dahua Technology Company (Dahua) (or their respective subsidiaries and affiliates) 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).[26] 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.[27]

11. In May 2025, the Commission adopted its *EA Integrity R&O and FNPRM*, in which we took steps, and proposed further steps, to promote the integrity and security of TCBs, measurement facilities (test labs), and laboratory accreditation bodies, which play an integral role in the Commission's equipment authorization program.[28] Specifically, it adopted a prohibition on FCC recognition of any TCB, test lab, or laboratory accreditation body owned by, controlled by, or subject to the direction of a prohibited entity (as defined by the *EA Integrity R&O and FNPRM*). These entities are barred from participating in our equipment authorization program, including both the equipment certification process and SDoC process.[29] To help ensure that the Commission has the necessary information to enforce this prohibition, the Commission expanded its reporting and certification requirements for all recognized TCBs, test labs, and laboratory accreditation bodies to certify to the Commission that they are not owned by, controlled by, or subject to the direction of a prohibited entity and to report all equity or voting interests of 5% or greater by any entity.[30] It also adopted amendments to the rules to state that the Commission will not recognize—and will revoke any existing recognition of—any TCB, test lab, or laboratory accreditation body that fails to provide, or that provides a false or inaccurate, certification; or that fails to provide, or provides false or inaccurate, information regarding equity or voting interests of 5% or greater.[31] In addition, it also clarified that our rules apply equally to all TCBs, test labs, and laboratory accreditation bodies regardless of the existence of MRAs or the physical location of the relevant facility. In the *EA Integrity R&O and FNPRM*, the Commission proposed and sought comment on further measures to safeguard the integrity of our equipment authorization program.[32] Namely, it sought comment on whether to extend the prohibitions to also include entities subject to the jurisdiction of a foreign adversary and whether to expand the group of prohibited entities to include several additional

[25] *Hikvision*, 97 F.4th at 950. While the court ordered a partial remand, it nonetheless rejected the petitioners' central claim that their equipment should not be on the Covered List at all. *See Hikvision*, 97 F.4th at 940 ("We hold that the [Secure Equipment Act] ratified the composition of the Covered List and leaves no room for Petitioners to challenge the placement of their products on that list under a predecessor statute.").

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

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

[28] *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Report and Order and Further Notice of Proposed Rulemaking, 40 FCC Rcd 3616 (2025) (*EA Integrity R&O and FNPRM*).

[29] *Id.* at 3617, para. 2.

[30] *Id*. at 3619, para. 5; *cf. Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control*, GN Docket No. 25-166, Notice of Proposed Rulemaking, FCC 25-28 (May 27, 2025) (proposing, *inter alia*, to adopt certification and information collection requirements for holders of Commission-granted licenses, authorizations, and other approvals that are owned by, controlled by, or subject to the jurisdiction or direction of, a foreign adversary).

[31] *Id.* at 3652, para. 77.

[32] *Id.* at 3619, para. 7.

lists from federal agencies or statutes.[33] It also sought further comment on ways the Commission can facilitate and encourage more equipment authorization testing to occur at test labs located within the United States or United States allied countries.[34] Finally, it sought further comment on post-market surveillance procedures to ensure compliance relating to prohibitions on authorization of covered equipment.[35]

III. DISCUSSION

12. In this Second R&O and Second FNPRM, we clarify and strengthen our existing prohibitions on covered equipment while also addressing and continuing to explore ways we can further strengthen the security of our supply chain through controls on importation and marketing.

A. Second Report and Order

13. In the Second Report and Order, the Commission clarifies that rules prohibiting authorization of covered equipment include modular transmitters and adopts a prohibition on authorization of devices that include modular transmitters that are covered equipment. The Commission also adopts a procedure to limit previously granted authorizations of covered equipment to prohibit the continued importation and marketing of such equipment. We further discuss the broad scope of the prohibition on authorization of equipment identified on the Covered List by clarifying the term "produced by" as used in our rules concerning covered equipment and clarifying the prohibition on modification to previously authorized covered equipment.

1. Prohibition on Modular Transmitters on the Covered List

14. In general, the Commission permits authorization of transmitters as standalone devices that can then be incorporated into a host device that may either rely on the authorization of that modular transmitter[36] or require its own additional authorization. Because modular transmitters are not required to obtain their own authorization as standalone devices, they can also be incorporated as a component in a host device that requires its own authorization. In this Second R&O, we clarify that our existing rules prohibiting the authorization of covered equipment include modular transmitters. We also now further prohibit the authorization of any device that includes a modular transmitter when that modular transmitter is itself covered equipment.[37] Under the existing attestation requirement, applicants and responsible parties will be required to attest that the subject equipment for which authorization is sought does not include such modular transmitters.[38] We find that these rule modifications advance both our national security objectives and the congressional directive to prevent the authorization of equipment that poses an unacceptable risk to national security.

15. *Background.* In the *EA Security NPRM* adopted in June 2021, the Commission proposed to require that applicants, when seeking equipment authorization, "attest that no equipment (including

[33] *Id.* at 3670-75, paras. 128-42.

[34] *Id.* at 3675-76, paras. 143-44.

[35] *Id.* at 3676, para. 145.

[36] 47 CFR § 2.903. Single modular transmitters consist of a completely self-contained radiofrequency transmitter device that is typically incorporated into another product, host, or device. Split modular transmitters consist of two components: a radio front end with antenna (or radio devices) and a transmitter control element (or specific hardware on which the software that controls the radio operation resides). All single or split modular transmitters are approved with an antenna. The term "modular transmitter" is defined in section 15.212 and includes single modular transmitters and split modular transmitters. *See* 47 CFR § 15.212(a).

[37] For example, we would prohibit authorization of a device that includes a modular transmitter that is equipment identified on the Covered List. *See id*.; Covered List.

[38] 47 CFR § 2.911(d)(5)(i).

component part) is comprised of any 'covered' equipment," as identified on the Covered List.[39] Many commenters opposed including an attestation requirement that considered component parts. In the subsequently adopted *EA Security R&O and FNPRM*, the Commission required that each applicant attest that the equipment for which it seeks authorization is not covered equipment,[40] but it declined at that time, based on the state of the record and the need for further consideration, to require that the applicant attestation address individual component parts contained within the applicant's equipment.[41] In declining to address component parts at that time, the Commission noted that it was seeking further comment on potentially including certain component parts within the scope of covered equipment.[42]

16. In seeking comment, the Commission "endeavor[ed] to ensure that equipment [ ] that include[s] component parts that pose an unacceptable risk to national security also be prohibited from authorization."[43] Accordingly, the Commission, noting many of the concerns that commenters raised,[44] sought comment on whether certain component parts, if included in equipment, would result in that equipment being covered equipment prohibited from authorization, and, if so, how the prohibition on the inclusion of any such component parts in equipment could be implemented in the Commission's equipment authorization program.[45] In particular, the Commission sought comment on whether it should attempt to identify components based on a risk assessment (e.g., examining whether the equipment contains components that are produced by entities identified on the Covered List and that process and retain data, or that only process data).[46] The Commission recognized that if it prohibited certain component parts, it would need to provide guidance on which components would be prohibited.[47]

17. The Commission focused much discussion on seeking comment on prohibiting authorization of equipment that incorporates as component parts certain types of modules produced by entities on the Covered List, whether authorized under the Commission's certification procedures or under the SDoC procedures.[48] As explained, the Commission permits specific types of modules–modular transmitters–to be authorized as "standalone" equipment under existing rules (provided the equipment meets all applicable Commission requirements).[49] A modular transmitter is a completely self-contained transmitter that only requires an input signal and power source to make it functional.[50] Commission rules provide that when an authorized modular transmitter is incorporated as a component part into another product,

[39] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket Nos. 21-232 and 21-233, Notice of Proposed Rulemaking and Notice of Inquiry (*EA Security NPRM*), 36 FCC Rcd 10578, 10600, para. 47 (2021).

[40] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13517-18, para. 54.

[41] *Id.* at 13519, para. 57.

[42] *Id.* at 13519, para. 57; *see id.* at 13599-606, paras. 268-287.

[43] *Id.*

[44] *Id.* at 13600-02, paras. 271-76.

[45] *Id.* at 13602-06, paras. 277-87.

[46] *Id.* at 13602, para. 279.

[47] *Id.* at 13602, para. 280.

[48] *Id.* at 13602-04, paras. 281-84.

[49] *Id.* at para. 281 & n.689 (when discussing modules, the Commission expressly cited its rules concerning "modular transmitters," 47 CFR § 15.212); *see* 47 CFR § 15.212 ("Modular transmitters"). For clarity purposes, we refer to these modules as "modular transmitters."

[50] *See EA Security R&O and FNPRM*, 37 FCC at 13602-03, para. 281 & n.689 (citing 47 CFR § 15.212 ("Modular transmitters")).

host, or device (e.g., composite systems,[51] personal computers), no further equipment authorization is required insofar as the final product, host, or device conforms to the terms of the module's authorization.[52] Considering these existing rules, the Commission further noted that telecommunications or video surveillance equipment could contain, as component parts, one or more such modular transmitters produced by entities identified on the Covered List, or could be assembled as a composite system and contain such equipment.[53]

18. The Commission specifically asked whether applicants (under certification procedures) and responsible parties (under SDoC procedures) should be required to use the Commission's equipment certification procedures to obtain an equipment authorization if the equipment or composite system includes, as a component part, a modular transmitter produced by an entity identified on the Covered List.[54] Further, the Commission inquired whether it should apply this equipment certification requirement to any equipment that incorporates, as a component part, a previously authorized modular transmitter produced by these entities (i.e., a modular transmitter authorized prior to adoption of the Commission's rules prohibiting authorization of covered equipment).[55] It also asked about potential additional costs in time and money that such approaches would impose on device developers.[56] Similarly, the Commission inquired whether composite systems should be treated in the same general manner as modular transmitters.[57] Relatedly, the Commission asked whether it should deem as covered equipment (and thus prohibited from authorization) any equipment that includes a component part that could be authorized as equipment on a standalone basis but for the fact that the standalone equipment would be prohibited from authorization as covered equipment.[58]

19. Further, the Commission asked for comment on the potential impact that prohibiting authorization of particular component parts (those that would be deemed covered equipment) would have on both equipment security and the economy.[59] Specifically, it sought comment and data on the effect of prohibiting particular component parts on the U.S. market (including quantity and market share of modules or other component parts that might be prohibited in products intended for sale in the U.S. market), the availability and costs of substitute modules, devices, and component parts from suppliers that are not identified on the Covered List, and the average lifespan/product cycle of affected final products.[60] It also inquired about the different impacts on both equipment security and the economy that would be expected depending on the breadth of the scope of a component part(s) prohibition.[61] In addition, the Commission generally sought comment on supply chain considerations, including whether the Commission should take into account how any prohibition of modular transmitters, if implemented

[51] A composite system incorporates different devices contained within a single enclosure or in separate enclosures connected by wire or cable. *EA Security R&O and FNPRM*, 37 FCC Rcd at 13602-03, para. 281 & nn.689, 692 (citing 47 CFR §§ 2.947(f) and 2.1033(e)); *see* 47 CFR §§ 2.947(f), 2.9033(e).

[52] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13602-03, para. 281. The presence of other transmitters in the device, or a change in device use of the previously authorized module in question, may require that the responsible party obtain additional equipment authorization(s) for the overall device. *See* 47 CFR part 2.

[53] *Id.* at 13602-03, para. 281.

[54] *Id*. at 13603, para. 282.

[55] *Id.*

[56] *Id.*

[57] *Id.* at 13603-04, para. 283.

[58] *Id.* at 13604, para. 284.

[59] *Id.* at 13606, para. 287.

[60] *Id.*

[61] *Id.*

immediately without advance notice or opportunity for the development of alternative sources of equipment, could have a deleterious effect on the public interest.[62]

20. The Commission received many comments on potentially including as covered equipment certain component parts produced by entities identified on the Covered List. Commenters include equipment and vendor associations, industry associations, U.S. equipment producers, consultants, producers of covered equipment, small businesses, and think tanks.[63] Most commenters either oppose including component parts in the prohibition on covered equipment or recommend that, if the Commission were to prohibit authorization of devices with certain covered component parts, it take only a narrow or targeted approach. CTA, ITI, NCTA, and USTelecom generally oppose extending covered equipment to include component parts, as do Hikvision and Dahua.[64] To the extent that the Commission were to prohibit certain component parts, CTA, CTIA, ITI, TIA, Competitive Carriers Association, USTelecom, and Verizon generally recommend that the Commission take a cautious and narrow approach while considering potential implementation and supply chain concerns.[65] Most commenters express concern about the difficulties associated with identifying the various components that equipment may include,[66] and about the potential supply chain disruptions and other potential unintended consequences

[62] *Id.* at 13612, paras. 309-10.

[63] Commenters include Consumer Technology Association (CTA) (around 1500 member companies that make up US consumer technology industry), Telecommunications Industry Association (TIA) (represents more than 400 global manufacturers and vendors of telecommunications equipment and services), Information Technology Industry Council (ITI) (global advocate for technology; an international trade association with professionals on 4 continents), American Council of Independent Laboratories (ACIL) (supports independent testing and certification across multiple industries), CTIA, NCTA – The Internet and Television Association (NCTA), NTCA, the Competitive Carriers Association, USTelecom – The Broadband Association (USTelecom), Motorola Solutions, Inc. (Motorola), Verizon Communications, Charles Parton, Horizon Advisory, Huawei, ZTE, Hikvision USA, Inc. (Hikvision), and Dahua Technology USA Inc. (Dahua), and think tanks, including the Foundation for Defense of Democracies and the Heritage Foundation.

[64] *See, e.g.*, CTA Comments at 7 (prohibition on equipment authorization for devices that contain certain component parts will burden innovators and consumers); CTA Reply Comments at 1-2 (urging the Commission to refrain from imposing further regulation on component parts); ITI Comments at 5-7 (recommending against the FCC exercising its authority to ban component parts; the Commission does not have legal authority to extend the prohibition on covered equipment to component parts); NCTA Reply at 6-9 (the FCC should limit prohibitions to finished products only and not to components or software); USTelecom Comments at 3 (components should generally not be considered in prohibition on covered equipment). *See* Hikvision Comments at 29-34; Dahua Comments at 5-8.

[65] *See, e.g.*, CTA Comments at 5-6 (the Commission should narrowly tailor any further changes to the equipment authorization regime to limit burdens and uncertainty); CTIA Comments at 6-14 (the Commission should be cautious about any regulations addressing component parts; any rules should be crafted to avoid unnecessary burdens on consumers and manufacturers); ITI Comments at 7; TIA Comments at 1-7 (urging a narrow and targeted approach, with focus only on components that pose a clear and compelling risk; expresses concern that actions could pose a significant risk of being overly burdensome and technically infeasible); TIA Reply at 4 (support only a targeted, risk-based approach, with clear and workable guidance); USTelecom Comments at 3 (argue that careful consideration should be given to impact on the market for finished products); Competitive Carriers Association Reply Comments at 8 (any new regulation should be narrowly tailored and only in response to clear national security risk); Letter from Nicolas Fetchko and Anita Patankar-Stoll, Verizon Communications, to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232 at 1-2 (rec. June 29, 2023) (Verizon June 29, 2023 *Ex Parte*) (future additions to the Covered List should be narrowly focused and aimed at addressing clear national security concerns).

[66] *See, e.g.*, ACIL Comments at 2-9 (particular equipment often includes many different component parts; it can be difficult for producers and assemblers, particularly small and medium sized enterprises, to know where modules might be sourced); CTA Comments at 7-8 (components are sourced from various companies and locations and tracking is a significant burden); ITI Comments at 6 (devices are comprised of many components sourced from many companies, and identifying the provenance of components can be administratively burdensome); NCTA Reply at 9. *See* Hikvision Reply at 20-21, 23.

that could occur due to a prohibition on component parts.[67] Several also note that industry groups are already working with the government in efforts to improve equipment security,[68] and many also advocate for a "whole of government" approach on addressing component parts.[69] Some also question whether the Commission has the requisite legal authority to prohibit the use of component parts in the covered equipment prohibition,[70] and some contend that other agencies should make determinations on whether component parts constitute covered equipment.[71] Several commenters state that, to the extent that the Commission were to prohibit particular component parts, the Commission would need to provide clear guidance identifying the specific component parts.[72] Some also recommend that the Commission work closely with industry prior to adopting rules to address particular components and establish an appropriate transition period if particular parts are deemed covered equipment.[73]

21. While the Commission requested comment on whether equipment containing certain component parts should be prohibited as covered equipment, most of those commenting provide only

[67] *See, e.g.*, ACIL Comments at 12; CTA Comments at 6, 9; CTA Reply Comments at 2 (argue that there would be an adverse impact on competition and innovation, supply chain disruptions, price increases, and potential harm to consumers); ITI Comments at 4-5 (note it is important to evaluate resiliency of supply chain for particular component parts); TIA Comments at 3-4; USTelecom Comments at 4-5 (such rules could disrupt supply chains and harm consumers); Competitive Carriers Association Reply at 6-7; Hikvision Comments at 30-36; Hikvision Reply at 21-22.

[68] *See, e.g.*, CTA Comments at 1-3; CTIA Comments at 2-4; USTelecom Comments at 1-3.

[69] *See, e.g.*, ACIL Comments at 8 (supports the Commission working with federal agencies in a whole-of-government approach); CTIA Comments at 4-6,8 (ICT security demands a whole-of-government approach, and national uniformity is critical; FCC should not attempt to identify ranges of components based on its own assessment, and instead should rely on whole-of-government effort); TIA Comments at 5 (the FCC should rely on a whole-of-government approach, along with consultation with industry). *Cf.* CTA Comments at 8-9 (FCC should not pursue developing its own standards that may be at odds with the national security agencies).

[70] *See, e.g.*, CTIA Comments at 8-9 (the Commission lacks statutory guidance on component parts and, under the Secure Networks Act and Secure Equipment Act, cybersecurity agencies have the authority to make judgments about what constitutes national security threats; the Commission may not be the proper entity to make these assessments and runs the risk of exceeding statutory authority); ITI Comments at 5-6 (the Commission's regulatory authority under the Secure Networks Act and Secure Equipment Act does not extend to component parts); Hikvision Comments at 29-30 (the Secure Networks Act and Secure Equipment Act do not apply to component parts); Dahua Comments at 5-6 (the Secure Networks Act and Secure Equipment Act do not apply to component parts).

[71] *See, e.g.*, CTA Comments at 8-9 (the Commission should not pursue its own standard); ITI Comments at 6 (the FCC should not prohibit component parts unless a clear and well-defined risk has been identified by the requisite national security agencies); TIA Reply at 4, 6 (the Commission should work with and rely upon national security agencies to identify specific component parts, and should not develop its own standards; urge selectively applying the Secure Equipment Act prohibitions to components based on clear and compelling determinations by the cybersecurity agencies). *Cf.* CTIA Comments at 8-9.

[72] *See, e.g.*, ACIL Comments at 6; TIA Comments at 6; CTIA Comments at 13; NCTA Reply at 8-9; Competitive Carriers Association Reply at 8; Verizon June 29, 2023 *Ex Parte* at 3 (the FCC must identify prohibited components with enough specificity to enable compliance). Some also note that CISA in its ICT SCRM Task Force has already begun efforts to develop a hardware bill of materials (HBOM), but that no HBOM had yet been developed. *See, e.g.*, CTIA Comments at 9-10 (the FCC should not duplicate work being done by the ICT SCRM Task Force on HBOM common taxonomy); ITI Comments at 8-10 (the FCC should be collaborating with CISA's efforts); NTCA Comments at 2-3 (the FCC should refrain from adopting rules governing expectations on components until the ICT-SCRM Task Force HBOM taxonomy becomes operational); NCTA Reply at 9-10. Several express concern that the Commission would require applicants and equipment manufacturers to create a "parts list." *See, e.g.,* ACIL Comments at 19; CTIA Comments at 7-8; ITI Comments at 8-10.

[73] *See, e.g.*, ACIL Comments at 8 (encourages the Commission to have more engagement with industry and the TCB Council before finalizing a rulemaking); TIA Comments at 6-7 (there should be a whole-of-government approach); Verizon June 29, 2023 *Ex Parte* at 2.

general, high-level feedback. The Heritage Foundation urges the Commission to "treat as 'covered communication equipment or service' any equipment that contains components that are a 'covered communications equipment or service.'"[74] Heritage further notes that Congress, in the Secure Networks Act, did not distinguish threats between "components and finished products."[75] Regarding approaches that focus on whether equipment that incorporates modules–such as modular transmitters–produced by entities identified on the Covered List, or composite systems that incorporate such modules, should be prohibited as covered equipment, ACIL states that the Commission's focus on these modules and composite systems "is a reasonable want," but also notes that there would be "several effects on the supply chain," including that it would be exceedingly difficult for some equipment producers (such as small- and medium-sized businesses) to know where the modules are sourced.[76] CTIA, TIA, and ITI note challenges associated with identifying the source of some modules.[77] TIA contends that modules have unique characteristics and should not be treated as posing the same security risks.[78] ITI states that defining modules would be challenging, and asserts that the Commission should not consider modules because of the complexity and difficulty of identifying the particular modules and because of the significant impact on innovation and supply chains; it further suggests that it should be left to the companies to assess whether components pose a risk.[79]

22. Several commenters highlight national security risks from components, especially modular transmitters. The Hudson Institute (Hudson) notes that devices incorporating "modular transmitters (from firms like Huawei and ZTE)," as well as a range of other components, can pose "the same national security threats" as devices produced directly by Huawei and ZTE.[80] The Heritage Foundation urges the Commission to take a maximalist approach and to "eliminate components and modules produced by foreign adversary entities from U.S. networks to the maximum extent permissible under its relevant authorities."[81] Heritage favorably cites the *EA Security R&O and FNPRM* to indicate that "components are fully capable of presenting risks to national security that are equally severe as risks from finished products."[82] Similarly, Horizon Advisory notes that the Chinese Communist Party is striving to "penetrate foreign [information systems] at the module and component level," which can give "Beijing access to the data flowing thorough these systems as well as the ability to disrupt them."[83] Moreover, such threats "can be more severe and pervasive than that stemming from downstream products" by granting access to the larger communications networks, allowing modules and components to serve as "beachheads through which the PRC expands its presence throughout the information and communications ecosystem."[84] Horizon notes that certain Chinese-produced modules enter into the U.S. market through supply relationships with original equipment manufacturers so that the devices carry a

[74] Bryan Burack Comments at 4 (rec. Aug. 25, 2025) (filed on behalf of The Heritage Foundation) (Heritage Comments).

[75] Heritage Comments at 4.

[76] ACIL Comments at 4-5.

[77] CTIA Comments at 10; TIA Comments at 2-4; ITI Comments at 7.

[78] TIA Comments at 3.

[79] ITI Comments at 6-7. *See id.* at 6 (identifying components is difficult; it would be extremely complex or practically impossible to create a list of modules and components to separately certify).

[80] Letter from David Feith and Michael Sobolik, Hudson Institute, to FCC, Docket No. ET 21-232, at 1 (filed Aug. 20, 2025 (Hudson *Ex Parte*).

[81] Heritage Comments at 4.

[82] Heritage Comments at 4.

[83] Horizon Advisory Comments at 2.

[84] Horizon Advisory Comments at 2.

trusted brand label on the outside, thereby presenting hidden risks.[85] Finally, Charles Parton submitted a report on cellular IoT modules that contends generally that certain Chinese-produced cellular modules, which, as part of IoT systems serve as the gateway for data transfer through 4G, 5G, and LTE networks, can pose security threats; Parton did not, however, comment directly on the specific proposals in the *EA Security R&O and FNPRM*.[86]

23. As for the Commission's request for comment on whether other components parts, if incorporated into equipment, would potentially raise unacceptable security risks such that relevant equipment should be prohibited from authorization, even fewer specific comments were proffered. ACIL expresses concern about what it terms "broad overreach" on component restrictions, and notes that prescriptive requirements on specific component parts, such as semiconductors, could paralyze whole industries; it recommends creating a group of industry experts to consider whether a device capable of examining an incoming or outgoing data stream and performing routing functions might be a good way forward.[87] ITI, however, opposes a "broad classification" for categories of component parts (e.g., RAM, CPU, etc.) or using "the extremely broad category" of "components that process or retain data," asserting that such a broad approach would not create sufficient clarity and would cause unnecessary confusion in supply chains. ITI acknowledges that the Commission has authority to prohibit equipment on the Covered List but contends that considering data management and routing issues may expand beyond that authority.[88] CTIA also expresses concern that a broad approach to component parts (or a parts list) would create a significant burden, and asserts that the component makeup of any given device may be proprietary and competitively sensitive.[89] Dahua also contends that a broad approach to component parts issues would raise serious practical concerns (*e.g.*, tracking the source of the parts, particularly by smaller manufacturers) and costs.[90] While TIA does not comment specifically on any of these other component parts, it states that any rule that would treat as covered any information and communications technology (ICT) device that contains any equipment produced by an entity identified on the Covered List would pose a significant risk of being overly burdensome to industry and technically infeasible given the realities of the ICT supply chain.[91]

24. Several commenters, including CTIA, ITI, TIA, and Verizon, recommend that, if the Commission were to conclude that equipment that includes certain modules or other component parts produced by entities on the Covered List is covered and thereby prohibited from obtaining an authorization, then the Commission should adopt a reasonable transition period to provide the necessary time to source replacements for the affected component part(s).[92] Finally, the Heritage Foundation also encourages the Commission to place on the Covered List component parts produced by a broad array of

[85] Horizon Advisory Comments at 3-4.

[86] *See generally* Charles Parton Report ("Cellular IoT modules – Supply Chain Security"). Parton is a consultant based in the United Kingdom.

[87] ACIL Comments at 6-7.

[88] ITI Comments at 7.

[89] CTIA Comments at 7.

[90] Dahua Comments at 8-9.

[91] TIA Comments at 4.

[92] *See, e.g.*, CTIA Comments at 10-11 (the Commission should provide industry with at least two years to find replacement parts); ITI Comments at 7 (the Commission should provide a "reasonable amount of time" to find a replacement module); TIA Reply at 5 (if the FCC extends covered equipment to include component parts, the FCC should provide ample time for manufacturers to source, test, and integrate new parts into their products); Competitive Carriers Association Reply at 8 (the FCC should allow a transition period of at least two years); Verizon June 29, 2023 *Ex Parte* at 2 (the FCC should engage in industry consultation to gather information regarding the transition periods necessary to implement any particular component ban; the transition period should be sufficient to allow the global market to adjust to avoid supply chain shortages).

"foreign adversary manufacturers," including Quectel and Fibocom, claiming that these components "present imminent national security risks."[93] While we lack independent authority to add these entities' equipment to the Covered List, we note, as does Heritage, that we have communicated with several of the enumerated sources about making Covered List determinations to consider risks from Quectel and Fibocom equipment.[94]

25. *Discussion.* Consistent with the potential approach on modules discussed in the *EA Security R&O and FNPRM*,[95] we conclude that any "modular transmitter" (as defined in section 15.212[96]) that is covered equipment is prohibited from authorization under our rules. Furthermore, we conclude that authorizing equipment that includes such a modular transmitter would effectively be authorizing the transmitter. As such, we prohibit from authorization any modular transmitter that is covered equipment, and any product, host, or device that incorporates a modular transmitter that is covered equipment, regardless of any previous authorization of the modular transmitter. This includes any transmitter identified on the Covered List that otherwise *could* be authorized as a module or on a standalone basis regardless of whether it *is* authorized. We believe this particular approach is necessary to ensure that modular transmitters that pose an unacceptable risk to national security or the safety and security of U.S. persons cannot be imported or marketed in the United States either as standalone devices or as incorporated into another device. And we believe that this approach ensures that we are addressing the national security threats that Congress intended for the Commission to address in the Secure Equipment Act, when it directed the Commission to not "approve any application for equipment authorization for [covered] equipment."[97]

26. Section 15.212 provides for a standalone authorization of modular transmitters under the Commission's certification procedures.[98] We conclude that modular transmitters, as defined in section 15.212, constitute communications equipment insofar as they are used in fixed or mobile broadband networks and provide high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction.[99] To the extent that a modular transmitter falls within the scope of what constitutes covered communications equipment under our rules,

[93] Heritage Comment at 5.

[94] Heritage Comment at 5; Letters from Debra Jordan, Chief, Public Safety and Homeland Security Bureau, and Ronald T. Repasi, Chief, Office of Engineering and Technology, FCC to Alan Estevez, Under Secretary, Bureau of Industry and Security, Department of Commerce, et al. (sent Sept. 1, 2023) https://docs.fcc.gov/public/attachments/DOC-396816A2.pdf.

[95] *Id.* at 13603, para. 282.

[96] 47 CFR § 15.212 (Modular transmitter).

[97] Secure Equipment Act § 2(a)(2).

[98] Commission rules provide that modular transmitters that have already been authorized can be installed as a component part in different equipment (e.g., composite systems, personal computers), and there is no general requirement under existing rules for a new equipment authorization to the extent that the equipment incorporates a previously certified module. However, limited modular approval may be granted for modules that only meet the rules when installed in particular product configurations. In such a case, additional certification requirements apply for installations that deviate from the original grant conditions.

[99] *See EA Security R&O and FNPRM*, 37 FCC Rcd at 13540-41, paras. 126-28; 47 CFR § 1.50001(a), (c). *See also EA Security R&O and FNPRM*, 37 FCC Rcd at 13569- 76, paras. 194-207 (discussing what constitutes "telecommunications equipment" for purposes of the Covered List and noting that "we interpret 'telecommunications equipment' as broadly as we previously defined 'communications equipment'").

the modular transmitter is itself covered equipment and thereby prohibited from authorization under our rules.[100]

27. Many modular transmitters are designed to be incorporated into equipment to enable that equipment to have certain critical or essential functionalities associated with the provision of fixed or mobile services. While such transmitters could be independently authorized, they are not required to be.[101] Given our conclusion that our rules prohibit from authorization standalone transmitters that fall within the scope of what constitutes covered equipment, we correspondingly prohibit from authorization equipment that includes, as a component part, a transmitter that meets the requirements for a modular transmitter, even if the transmitter is not independently authorized as a module.[102] This approach is consistent with the Commission's suggested approach in the *EA Security R&O and FNPRM* to prohibit authorization of any equipment that includes a component part that could be authorized on a standalone basis but for the fact that the standalone equipment would be prohibited from authorization.[103] Because this communications equipment is covered equipment, preventing authorization of equipment that includes this covered equipment is necessary and appropriate, and consistent with the Commission's authority under the Act, the Secure Networks Act, and the Secure Equipment Act to prohibit authorization of equipment that poses an unacceptable risk to national security, and covered equipment more specifically. That is, we conclude that granting an authorization for equipment that includes a modular transmitter that is covered equipment would, in effect, be granting an authorization to equipment that, by inclusion of this covered modular transmitter, would pose an unacceptable risk to national security and would undermine Congress's goals in the Secure Equipment Act when it directed the Commission to cease authorizing covered equipment.[104] We agree with the Heritage Foundation that such equipment can "present[] risks to national security that are equally severe as risks from finished products."[105] Authorizing devices containing one or more covered modular transmitters is tantamount to authorizing the modular transmitter(s). It makes little sense for the Commission to prohibit certain modular transmitters from obtaining independent authorization, but to allow authorization for devices containing exactly those modular transmitters.[106]

28. We therefore modify our rules to explicitly prohibit authorization of any modular transmitter that is covered equipment, and any product, host, or device that incorporates a modular transmitter that is covered equipment, regardless of whether the Commission previously authorized that modular

[100] 47 CFR §§ 2.903(a), 1.50001(d). Among the comments the Commission received, Charles Parton, a consultant based in the United Kingdom, submitted a report on cellular IoT modules that contends generally that certain Chinese-produced cellular modules, which as part of IoT systems serve as the gateway for data transfer through 4G, 5G, and LTE networks, can pose security threats. *See* Charles Parton Report. While he did not comment directly on this proceeding, we note that cellular IoT modules would fall within the scope of modular transmitters under Commission rules. *Id*. Furthermore, IoT devices are often telecommunications equipment. *EA Security R&O and FNPRM* at para. 201.

[101] *See* 47 CFR § 15.212.

[102] In light of Charles Parton's report in our record, which contends generally that certain Chinese-produced cellular modules, which as part of IoT systems serve as the gateway for data transfer through 4G, 5G, and LTE networks, can pose security threats, *see generally* Charles Parton Report, we note that cellular IoT devices would fall within the scope of modular transmitters under Commission rules.

[103] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13604, para. 284.

[104] Secure Equipment Act § 2(a)(2).

[105] Heritage Comments at 4.

[106] In this sense, we agree with the Hudson Institute that continued authorization of devices that contain these modular transmitters "undermine the intent of" the Secure Networks Act and the Secure Equipment Act. Hudson *Ex Parte* at 4.

transmitter. Modular transmitters, as defined in section 15.212 of the Commission's rules,[107] that can be authorized under our rules as standalone devices (each consisting of a completely self-contained transmitter device) and incorporated into other devices,[108] include "single-modular transmitters," "split-modular transmitters," and "limited modular transmitters."[109] We also include in our prohibition modular transmitters that operate pursuant to licensed radio services rules.[110] We conclude that this prohibition furthers the objectives of our equipment security rules, as well as the congressional directive to prohibit authorization of equipment that poses an unacceptable risk to national security.[111]

29. We reject the contention of some commenters either that the Commission may not have the requisite legal authority to prohibit use of any component parts[112] or that only the enumerated sources identified in the Secure Networks Act should make determinations on whether component parts constitute covered equipment.[113] First, the only component parts that the Commission is prohibiting with the rules announced today are those that are themselves covered equipment, which have already been determined to pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons."[114] While the Commission lacks independent authority to add new equipment to our Covered List without the specific determination of an enumerated source or direction from Congress,[115] we conclude that the Commission has the requisite RF equipment expertise to reach the conclusion that whatever unacceptable risks are posed by modular transmitters are posed regardless of whether those modular transmitters are initially approved as standalone devices or incorporated within a product, host, or device, as modular transmitters are generally intended to be. In issuing this prohibition, the Commission is not making impermissible national security determinations. The Commission is rather using its decades-long technical expertise concerning RF equipment and familiarity with its equipment authorization process to close a loophole that would undermine both the Secure Equipment Act's directives and Congress's and the Executive Branch's determinations as to national security risks.

---

[107] 47 CFR 15.212. We note that in our part 2 and part 15 rules associated with the Commission's equipment authorization program, the term "modular transmitters" is only used in section 15.212. The general term "modules" is not used in our rules, though there is occasional reference to "modular" components (*e.g.*, sections 15.102, 2.1077(b)).

[108] Under our existing rules, if a modular transmitter is authorized as a standalone device, it could obtain an FCC identification number. *See* 47 CFR §15.212(a)(1)(iv)(A)-(B), (2). And, under our existing rules (and KDB guidance), this modular transmitter could be installed in other equipment without additional authorization. If a certified module is used for its approved intended end use and follows the module integration instructions, it does not need to be retested before being installed and marketed in a host device not subject to certification itself, creating a potential loophole that the rules we adopt today would close. The Commission KDB publication guidance for modules is KDB 996369.

[109] *See* 47 CFR § 15.212.

[110] *See* KDB 996369 D01 Module Certification Guide v03, section 2 (KDB 996369).

[111] In adopting rules to prohibit use of modular transmitters in equipment for which authorization is sought, we are in effect prohibiting composite systems that include modular transmitters that are covered equipment.

[112] *See, e.g.*, CTIA Comments at 8-9; ITI Comments at 5-6; Hikvision Comments at 29-30; Dahua Comments at 5-6.

[113] *See, e.g.*, CTA Comments at 8-9 (the Commission should not pursue its own standard); ITI Comments at 6 (the FCC should not prohibit component parts unless the requisite national security agencies have identified a clear and well-defined risk); TIA Reply at 4, 6 (the Commission should work with and rely upon national security agencies to identify specific component parts, not develop its own standards, and only selectively apply the SEA prohibitions to components based on clear and compelling cybersecurity agency determinations). *Cf.* CTIA Comments at 8-9.

[114] 47 U.S.C. § 1601(b); 47 CFR § 1.50002(b)(1).

[115] 47 U.S.C. § 1601(b); 2025 NDAA § 1709(a)(2).

30. Second, the Secure Equipment Act directed the Commission to "adopt rules in the [*EA Security NPRM* proceeding]."[116] Congress thus directed the Commission to adopt final rules in a proceeding which had proposed to require that applicants "attest that no equipment (including component parts) is comprised of any 'covered' equipment, as identified on the [Covered List]."[117] Had Congress (incongruously) intended for the Commission to *not* authorize certain covered equipment but *to* authorize devices containing covered equipment, Congress could have prohibited the Commission from addressing components parts, as proposed. Congress chose not to.

31. Third, even in the absence of the Secure Equipment Act, we conclude that the Commission possesses sufficient legal authority under the Act to implement the prohibitions contained in this section.[118] As explained in the *EA Security R&O and FNPRM*, section 302 of the Act authorizes the Commission to make regulations "consistent with the public interest, convenience, and necessity…governing the interference potential of [radio frequency] devices."[119] This public interest regulatory authority implicates other statutory responsibilities, including the missions for which the Commission was created–promoting national defense and the safety of life and property; interests clearly furthered by prohibiting the importation and marketing of devices that pose "unacceptable risks to the national security of the United States or the safety and security of United States persons."[120] Other statutory authorities confirm this.[121] If there was any doubt that the Commission possessed this pre-existing authority, Congress confirmed it with the Secure Equipment Act. The Secure Equipment Act's direction of Congress to adopt rules in the *EA Security NPRM* ratified the Commission's tentative legal conclusions and decisively established the Commission's legal authority to enact the proposals in the *EA Security NPRM*, one of which was to require attestation as to component parts.[122]

---

[116] *See* Secure Equipment Act § 2(a)(1).

[117] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket Nos. 21-232 and 21-233, Notice of Proposed Rulemaking and Notice of Inquiry (*EA Security NPRM*), 36 FCC Rcd 10578, 10600, para. 47 (2021).

[118] *See EA Security R&O and FNPRM*, 37 FCC Rcd at 13511-13513, paras. 40-43 (describing the Commission's pre-Secure Equipment Act legal authority to prohibit equipment in the event that a national security agency determines that the equipment poses an unacceptable risk to our national security). Additionally, even if a device containing one or more modular transmitters that would be prohibited from receiving authorization as covered equipment was not itself covered equipment, the Commission would possess the authority to make a reasonable technical judgment that such equipment poses the same risks as covered equipment and thus extend the prohibitions to such equipment. *See id.*; 47 U.S.C. §§ 151, 302a(a) (broadly granting the Commission the authority "consistent with the public interest, convenience, and necessity, [to] make reasonable regulations … governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications").

[119] 47 U.S.C. § 302a(a); *EA Security R&O and FNPRM*, 37 FCC Rcd at 13511, para. 40.

[120] 47 U.S.C. § 1601.

[121] *See, e.g.*, 47 U.S.C. § 303(g) (authority to "generally encourage the larger and more effective use of radio in the public interest"); 47 U.S.C. § 303(e) (authorizing the Commission to "[r]egulate the kind of apparatus to be used with respect to 'its external effects'" among other things); 47 U.S.C. § 303(r) (authority to adopt rules "as may be necessary to carry out the provisions of [the] Act"); 47 U.S.C. § 154(i) (providing the Commission with ancillary authority to implement these statutory provisions "as may be necessary in the execution of [previously-described] functions.").

[122] *EA Security NPRM*, 36 FCC Rcd at 10600, para. 47; *EA Security R&O and FNPRM*, 37 FCC Rcd at 13512, para. 42 ("Our reading of the Commission's pre-enactment authority is confirmed by Congress's enactment of the Secure Equipment Act. … Congress clearly intended to ratify the Commission's tentative conclusions in the *NPRM* that it had authority as discussed therein.").

2. Limitation on Existing Authorization of Covered Equipment

32. We set forth a process to place limitations on previously granted authorizations of covered equipment to prohibit the continued importation and marketing of such equipment. Through this approach, the Commission aims to effectively address the established national security risks posed by previously authorized covered equipment while minimizing the impact on users. Our goal is to mitigate potential national security risks associated with covered equipment that was authorized prior to adoption of the *EA Security R&O and FNPRM* in November 2022.

33. *Background*. In the *EA Security R&O and FNPRM*, the Commission adopted a prohibition on the authorization, going forward, of covered equipment, and concluded that it has the requisite legal authority under the Act, confirmed by the Secure Equipment Act, to revoke existing authorizations, but it did not at that time revoke any existing authorizations.[123] The Commission also adopted streamlined revocation procedures for equipment authorizations granted after adoption of the prohibition if the applicant included a false statement or representation that the equipment for which it had sought and obtained a grant is not "covered" equipment.[124] The Commission sought further comment on the issues raised in the *EA Security NPRM* concerning revocation of covered equipment authorizations granted prior to the Commission's adoption of a prohibition on authorization of such equipment.[125] It sought to expand the record that developed in response to the *EA Security NPRM*, particularly in light of the actions taken and guidance provided in the *EA Security R&O and FNPRM*, and sought comment on several different issues concerning revocation.

34. Specifically, the Commission sought comment on the scope of revocation of existing authorizations the Commission should consider, whether there might be situations that would warrant revocation in certain circumstances and, if so, how the Commission should identify particular covered equipment for which continued authorization poses an unacceptable risk to national security.[126] Further, considering the potential risk to national security, it asked whether the Commission should consider revoking all existing authorizations of covered equipment and, if so, how such revocations could be implemented. The Commission also asked to what extent revocation of any particular equipment should depend on establishing a reimbursement program.[127] It also inquired how supply chain issues or consumer-related concerns should figure into the Commission's considerations, and what information and data might be useful to such a consideration.[128] The Commission requested comment on an appropriate transition period in the event that the Commission were to decide to revoke any existing authorizations of covered equipment.[129] In addition, the Commission sought comment on what process to use for revocation of existing authorizations, and whether it should adopt different or expedited procedures than provided for under section 2.939 of the Commission's rules.[130] Further, the Commission asked about the best enforcement mechanisms of any revocation, such as an enforcement policy to address violations related to the continued marketing, sale, or operation of covered equipment for which authorization was

[123] *EA Security R&O*, 37 FCC Rcd at 13535, para. 107.

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

[125] *See generally EA Security R&O and FNPRM*, 37 FCC Rcd at 13606-12, paras. 288-308.

[126] *Id.* at 13607, 13608-09, paras. 291-92, 295.

[127] *Id.* at 13608-09, para. 295.

[128] *Id.* at 13609-10, paras. 298-99.

[129] *Id.* at 13609, para. 296.

[130] *Id.* at 13611, 13612, paras. 303-04, 307.

revoked.[131] The Commission asked what educational and outreach efforts may be needed to inform the public of any revocations of covered equipment authorizations.[132]

35. The Commission also requested comment on possible alternative approaches to full revocation of existing authorizations. It sought comment on what it termed a "partial" revocation by which the continued importation and marketing of previously authorized covered equipment would be prohibited without impacting the continued use of such equipment.[133] The Commission noted that such an approach could eliminate user device replacement costs while also promoting national security concerns related to the continued importation and marketing of this equipment.[134]

36. Commenters, including CTA, CTIA, TIA, Competitive Carriers Association, and NCTA generally oppose any widespread revocation of existing authorizations of covered equipment that would require removal and replacement of equipment in use,[135] while other commenters, including ITI, ZTE, Hikvision, and Dahua, contend that any revocation of existing authorizations is precluded by the Secure Equipment Act[136] or otherwise would violate due process.[137] Several of these commenters contend that revocation of all existing authorizations of covered equipment would be costly and raise significant practical and feasibility concerns,[138] would create a variety of complexities and uncertainties,[139] including

[131] *Id.* at 13611-12, paras. 305-06.

[132] *Id.* at 13612, para. 308.

[133] *Id.* at 13610, para. 300.

[134] *Id.*at 13610, para. 300.

[135] CTA Comments at 10-12; CTIA Comments at 14-18; TIA Comments at 7; Competitive Carriers Association Reply at 2-6; NCTA Reply at 3-6.

[136] *See, e.g.*, ITI Comments at 2-3 (asserting that the Secure Equipment Act expressly precludes FCC from retroactive revocation); Dahua Comments at 10-11; Hikvision Comments at 5-6. These comments misread the Secure Equipment Act by omitting discussion of the "Rule of Construction" clarifying that the Secure Equipment Act does not prohibit the Commission from revoking authorizations for covered equipment in future actions, Secure Equipment Act § 2(a)(3)(B), such as this one. ITI also twice misquotes the Secure Equipment Act in ways that would advance ITI's preferred outcome. Per ITI, the Secure Equipment Act reads: "Retroactivity: The rules adopted by the FCC may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the list described above." ITI Comment at 2, 2-3. However, the provision that ITI apparently is referring to makes no reference to "retroactivity" and only expressly prohibits the Commission from reviewing or revoking equipment authorizations in the rules enacted as a result of the *EA Security NPRM*. *See* Secure Equipment Act § 2(a)(3)(A) ("In the rules adopted under paragraph (1), the Commission may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the list described in paragraph (2)."). Instead, the Secure Equipment Act expressly acknowledges the Commission's pre-existing authority to engage, review, or revoke any equipment authorization for covered equipment in subsequent proceedings. *Id.* § 2(a)(3)(B) ("Rule of construction.—Nothing in this section may be construed to prohibit the Commission other than in the rules adopted under paragraph (1), from—(i) examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the [Covered List]; or (ii) adopting rules providing for any such review or revocation.").

[137] *See, e.g.*, ZTE Comments at 3; Hikvision Comments at 4-19 (the Commission has no legal authority and such action would be arbitrary and capricious.); Dahua Comments at 18-19 (such action would violate the Administrative Procedure Act and due process under the Constitution.).

[138] *See, e.g.*, ACIL Comments at 14; Hikvision Comments at 16-17; NCTA Reply at 3.

[139] *See, e.g.*, NCTA Reply at 3 (could seriously disrupt the marketplace, undercut consumer reliance on part 2 authorizations, and place disproportionate burden on network operations); Dahua Comments at 7-8; Competitive Carriers Association Reply at 3 (would create undue complexity and confusion).

determining which equipment authorizations would be revoked,[140] would harm consumers,[141] and would raise significant due process concerns.[142] Some contend that equipment life cycles should be taken into account,[143] while others emphasize the costs that would be associated with requiring equipment to be replaced, contending that reimbursement mechanisms would need to be established.[144] Some assert that innovation would be stifled.[145] Several also state the need for a transition period that takes into account supply chain considerations, which could be as long as a few years.[146] Some raise enforcement concerns[147] and potential international trade concerns.[148] Dahua and Hikvision each contend that the Commission should consider alternatives to revocation that are less burdensome,[149] while ZTE asserts that revocation of existing authorizations is unnecessary as such equipment will exit the market simply by operation of the market itself as older devices become obsolete and are replaced with newer devices.[150]

37. CTIA contends that revocation, if not based on a limited and prospective approach, should only be reserved for extraordinary cases where the national security agencies specifically ask the Commission to revoke the authorization. It also argues that any such revocations should be subject to a formal hearing, include a phase-out period, and that the Commission should provide guidance for alerting consumers.[151] TIA contends that the Commission should reserve any revocation of existing authorizations for cases of extreme concern. TIA further asserts that any such revocation must serve critical national security interests significant enough to outweigh the substantial burden on industry and consumers, and should not occur without a fund to cover reimbursement and replacement costs.[152] CTA contends any

[140] *See, e.g.*, ITI Comments at 3 (noting significant implementation concerns, including the difficulties of determining which grants of authorization to revoke and require replacement, as well as consumer confusion).

[141] *See, e.g.*, CTIA Comments at 14; Competitive Carriers Association Reply at 2; TIA Reply at 3.

[142] *See, e.g.*, CTIA Comments at 16; ITI Comments at 4; NCTA Reply at 16; Hikvision Reply at 17.

[143] *See, e.g.*, ACIL Comments at 12; TIA Reply at 3 (typical lifespan of equipment is three to five years).

[144] *See, e.g.*, CTA Comments at 10-11 (arguing that replacement costs would harm consumers and involve difficulties in identifying cost-effective replacements.); CTA Reply at 2 (if revoked, the Commission would need realistic transition and funding mechanisms for equipment replacement); CTIA Comments at 14-18 (any revocation would create serious complications and harm consumers, and should be limited and prospective, and promote due process); ITI Comments at 3 (unclear which entity would bear responsibility for ensuring compliance, or have the liability for replacement parts and replacement); NCTA Reply at 6; USTelecom Comments at 5 (reimbursement); Hikvision Comments at 23-24; *cf.* Dahua Comments at 11-13.

[145] *See, e.g.*, Hikvision Comments at 25; Dahua Comments at 17; ITI Comments at 2.

[146] *See, e.g.*, CTA Comments at 10-11 (urging a minimum of 2 years); CTIA Comments at 16; USTelecom Comments at 7; Competitive Carriers Association Reply at 2; NCTA Reply at 6 (urging a reasonable transition period with sufficient time to source and replace equipment); Dahua Comments at 21.

[147] *See, e.g.*, Dahua Comments at 14-15 (stating difficulty of tracking down equipment or dealers/distributors that possess the authorized equipment).

[148] *See, e.g.*, USTelecom Comments at 8; Dahua Comments at 16-17 (revoking authorization of previously approved equipment through mutual recognition agreements (MRAs) could create uncertainty and delays in global trade and disrupt supply chains).

[149] Dahua Comments at 18 (alternatives could include compliance programs in collaboration with the Commission; voluntary recall of noncompliant equipment; development and enhancement of industry standards, guidelines, and best practices; implementing regular compliance monitoring and reporting programs; including use restrictions on existing equipment; and improving cybersecurity of devices); Hikvision Comments at 27-28 (alternatives include the use of labels, software patches, and other cybersecurity best practices).

[150] ZTE Comments at 5-6.

[151] *See* CTIA Comments at 14-18.

[152] TIA Comments at 7-8.

such revocation should occur only in limited circumstances where necessary, after consultation with national security agencies as well as a robust public process, and then only if there is a realistic transition period and a funding mechanism for equipment replacement.[153] The Competitive Carriers Association also contends that the Commission should limit any such revocation to only extraordinary circumstances based on evidence of real, discernable benefit to national security and take into account ways to minimize negative and unintended consequences, and that carriers and consumers should not bear the costs of any "rip and replace" initiatives associated with such revocation.[154] NCTA argues that the Commission should carefully consider any revocation of existing authorizations and, if not prospective only, base such revocation on extraordinary circumstances and upon a specific national security agency finding that such revocation is necessary for national security, pursuant to due process, and include a funding mechanism and a reasonable transition period to allow providers to source and replace equipment.[155]

38. Some commenters are supportive of a broad revocation of covered equipment authorizations. The Heritage Foundation urges the Commission to review previously authorized covered equipment and to "revoke equipment authorizations from entities that have subsequently been identified on the Covered List," noting the thousands of equipment authorizations the Commission has granted for equipment that is now covered.[156] Heritage asserts that because "these entities have already been determined to present unacceptable national security risks, their equipment has no place in U.S. critical infrastructure, on store shelves, or anywhere subject to the Commission's jurisdiction where it could be leveraged to compromise Americans' safety or privacy."[157] Furthermore, the Foundation for Defense of Democracies (FDD) notes that "[e]quipment authorized before February 6, 2023, has the same, or nearly identical, technical capabilities that make newly banned devices dangerous" and so should not be treated differently from new equipment.[158] Similarly, Hudson notes that the FCC should not rely on natural obsolescence of equipment to eliminate risks and urges the Commission to "[e]stablish a process for revoking authorization of Covered List equipment."[159] Finally, Horizon Advisory urges the Commission to "engage in revocations" of "already-authorized 'covered' equipment," given the threat such equipment poses.[160]

39. Finally, some commenters state that, apart from retroactive revocation of existing authorizations (including prohibiting continued use of equipment) or revocation of authorizations of specific equipment based on extraordinary circumstances, the Commission could consider some form of prospective approach to revocation of covered equipment that would prohibit the future marketing or sale of currently authorized covered equipment. For instance, CTIA states as a general matter that, except in

[153] CTA Reply at 2. In its comments, CTA contends that the Commission should exercise revocation of devices containing prohibited components only in extraordinary circumstances and only on a case-by-case basis after specific national security agency determinations. CTA Comments at 11.

[154] Competitive Carriers Association Reply at 5. In the *Supply Chain Second R&O*, the Commission required removal and replacement of covered telecommunications equipment produced by Huawei and ZTE and purchased with Universal Service Funds for use in networks. *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain Second R&O*).

[155] NCTA Reply at 3-6.

[156] Heritage Comments at 3.

[157] Heritage Comments at 3.

[158] FDD Comments at 3. The Commission notes that, concurrent with release of the *EA Security R&O and NPRM* (Nov. 25, 2022), it adopted an interim freeze on further processing or grant of equipment authorization applications for equipment produced by any entity identified on the Covered List as producing covered equipment. *EA Security R&O and NPRM*, 37 FCC Rcd at 13589, para. 264.

[159] Hudson *Ex Parte* at 4.

[160] Horizon Advisory Comments at 5.

extraordinary cases, the Commission should favor a limited and prospective approach to revocation, citing the Commission's discussion of a partial and limited revocation prohibiting future sale and importation of covered equipment that would reduce future risk while also minimizing the challenges associated with trying to remove existing devices from consumer hands;[161] CTIA notes that such an approach also would avoid arguments about retroactive application.[162] The Competitive Carriers Association urges caution about a revocation approach and, as a potential alternative, notes that the Commission "could prohibit the prospective purchase of covered equipment whose authorization has been revoked but 'grandfather' equipment and devices already in the marketplace," or it could permit a transition period for the duration of the reasonable life of the equipment.[163] NCTA asserts that "revocations should presumptively be prospective only," which it states would reduce due process concerns and minimize the impact on consumers and network operators.[164] Although CTA does not propose that the Commission take some form of prospective approach, it argues that, if the Commission were to take action to prohibit new sales going forward, the operation of existing previously authorized devices should be allowed to continue.[165] The Heritage Foundation conversely argues for sweeping revocations, but, in the alternative, encourages the Commission to "[a]t a minimum" take a prospective approach in which "further importation and marketing of [covered] equipment should be brought to an end."[166]

40. *Discussion*. To promote our goal of mitigating the national security risks associated with previously authorized covered equipment in our nation's infrastructure and communications supply chain, we adopt a procedure whereby the Commission can limit previously granted authorizations of covered equipment to prohibit the continued importation and marketing, without prohibiting the continued use of such devices. This is a simplified, prospective approach along the general lines of the prospective "partial" revocation proposal on which the Commission sought comment in the *EA Security R&O and FNPRM* that would not affect consumers' continued use or operation of devices they already possess.[167] Absent a process by which we can restrict the continued importation and marketing of covered equipment, we are concerned that already-authorized covered equipment devices would continue to flow into our nation and into our infrastructure and communications supply chain, which could contribute to further unacceptable risks. These devices have been determined to pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons" alongside all other covered equipment.[168] We further conclude that it is insufficient to rely solely on the obsolescence of particular equipment models to abate the inflow of more covered equipment. Years-old covered devices are still widely sold in the U.S., suggesting obsolescence is not a quick process.[169] Older models

[161] CTIA Comments at 15 ("limited, forward looking revocations would … avoid arguments about retroactive revocation").

[162] Short of a prospective approach, CTIA contends that the Commission should only consider revoking covered equipment authorizations if the equipment violates the rules in place at the time it was initially approved and marketed. *Id.* at 16.

[163] Competitive Carriers Association Reply at 2, 6.

[164] NCTA Reply at 6; *see generally id.* at 3-6 (any rules permitting revocation of an existing authorization should be carefully calibrated and, absent extraordinary circumstances, prospective only).

[165] CTA Comments at 11. *Cf.* TIA Comments at 6 (although specifically discussing any prohibition on component parts, TIA states generally that "any rules adopted in this proceeding apply only in a prospective manner and include reasonable, workable timelines for the industry").

[166] Heritage Comments at 3.

[167] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13610, para. 300.

[168] 47 U.S.C. § 1601(b)(1).

[169] *See, e.g.,* ebay.com, Huawei Port Wireless Routers 1, https://www.ebay.com/b/Huawei-Port-Wireless-Routers-1/44995/bn_106264985 (Sept. 30, 2025).

of covered equipment poses an unacceptable risk today when imported or marketed in the United States, not only when such equipment is new to the market. Waiting many years for this equipment to become obsolete would not address the present "unacceptable risks. We agree with the Heritage Foundation that certain previously authorized devices that are now considered covered equipment "likely remains marketable in the United States" and "may present continuing national security threats."[170] Furthermore, as FDD noted, such devices, embedded within American communications networks, "can still undergo firmware updates, conduct remote communication, and transmit data back to their manufacturers."[171]

41. In the *EA Security R&O and FNPRM*, the Commission concluded that it has the requisite authority under the Act to review any existing authorization for covered equipment, and to determine the necessity for revoking such authorization, and that the Commission can undertake such revocation pursuant to current rules.[172] Under its current rules in section 2.939(a), the Commission has already established procedures to revoke an equipment authorization because of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application.[173] In the case of previously authorized covered equipment, the implementation of the Covered List and the resulting prohibition on authorization of equipment identified on the Covered List create conditions that would warrant the Commission in refusing to grant an original application for any covered equipment.[174] The Commission does not today alter our existing process to revoke covered equipment, as proposed in the *EA Security R&O and FNPRM*, which in most cases involve the process generally afforded radio licenses.[175] Instead, the Commission adopts a new process well-tailored to address unacceptable national security risks without disrupting continued use or operation of devices.

42. We revise the Commission's rules to adopt a procedure to limit the scope of an existing authorization of covered equipment to prohibit continued importation or marketing of such equipment, without revoking the underlying authorization. The Commission has in various proceedings adopted prohibitions on the manufacture and importation of equipment where doing so served the public interest.[176] Section 302 of the Act authorizes the Commission—consistent with the public interest, convenience, and necessity—to promulgate regulations applicable to the manufacture, import, sale, offer for sale, shipment, and use of radiofrequency devices and to prohibit the manufacture, import, sale, offer for sale, shipment, or use of such devices that fail to comply with those regulations.[177] Consistent with our existing regulatory procedures to revoke an equipment authorization, we find, through this rulemaking proceeding, the Commission has the requisite authority to evaluate, craft, and implement this process to limit the scope of an existing authorization of covered equipment to prohibit continued

[170] Heritage Comments at 3.

[171] FDD Comments at 3.

[172] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13537, para. 114.

[173] 47 CFR § 2.939(a)(4).

[174] *See* 47 CFR §§ 1.50002, 2.903.

[175] 47 CFR § 2.939(b).

[176] *See, e.g.*, *Amendment of Parts 1, 2, 15, 90 and 95 of the Commission's Rules to Permit Radar Services in the 76-81 GHz Band*, ET Docket No. 15-26, Report and Order, 32 FCC Rcd 8822 (2017) (prohibiting certification of wideband vehicular radars designed to operate in the 22.12-29 GHz and ultra-wideband vehicular radars designed to operate in the 22-29 GHz band, and prohibiting the manufacture, importation, marketing, sale, and installation of such devices after a specified date); *Amendment of Parts 2 and 15 of the Commission's Rules to Further Ensure that Scanning Receivers Do Not Receive Cellular Radio Signals*, ET Docket No. 98-76, Report and Order, 14 FCC Rcd 5390 (1999) (banning the importation and manufacture of certain scanning receiver and frequency converter kits); *Amendment of Parts 2 and 15 to Prohibit Marketing of Radio Scanners Capable of Intercepting Cellular Telephone Conversations*, ET Docket No. 93-1, Report and Order, 8 FCC Rcd 2911 (1993) (requiring the manufacture or importation of scanning receivers and frequency converters after a specified date).

[177] 47 U.S.C. § 302a(b).

importation and marketing of such equipment, and to establish a procedure to apply this limitation as appropriate.[178] Our action is consistent with "the public interest" insofar as it protects American communications networks from devices specifically determined to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[179]

43. While commenters generally oppose widespread revocation of existing authorizations of covered equipment, several commenters recommend that, instead of widespread revocation of existing authorizations, or revoking particular authorizations because of "extraordinary" circumstances, the Commission should take a prospective approach to addressing existing authorizations along the lines suggested in the *EA Security R&O and FNPRM*,[180] under which the Commission would only consider whether to prohibit in some manner the future importation and marketing of previously authorized covered equipment while allowing the continued operation of equipment already in use.[181] This allows the Commission to avoid the "[e]conomic harms associated with removing and replacing Covered List equipment."[182] We agree, and adopt such an approach in this Second R&O—limiting equipment authorizations to prohibit importation and marketing, while allowing for continued operation of the relevant devices.

44. We revise section 2.939 of our rules by adopting a mechanism to limit the continued importation and marketing of such previously authorized covered equipment. We delegate authority to OET and PSHSB to apply such prohibitions pursuant to the framework and process that we describe here. We revise our section 2.803 and 2.1204 rules to clarify that equipment that has been subject to such a limitation cannot be marketed or imported.

45. For such previously authorized covered equipment, OET and PSHSB shall provide, through public notice, a brief analysis of the relevant factors that would justify limitation on the authorization of previously authorized covered equipment prohibiting the importation and marketing of such. In each such public notice, OET and PSHSB will specify the class, type, or other description sufficient to identify the devices, including reference to all devices included in a specific Covered List entry, targeted for

---

[178] Zhejiang Dahua argues that the Secure Equipment Act does not afford the Commission any new authority to revoke or limit authorizations that it did not have before enactment of that statute. Zhejiang Dahua further asserts that the proposed limitation on importation and marketing are "unrelated to the Commission's authority to prevent interference and therefore not permitted by statute." Letter from Andrew D. Lipman, Counsel to Zhejiang Dahua Technology Co. Ltd. to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232, at 2 (filed Oct. 20, 2025) (Zhejiang Dahua *Ex Parte*). Despite these arguments, we do not here claim any new authority to revoke or limit equipment authorizations. The adoption of this new procedure is consistent with our existing authority to revoke equipment authorizations and provides a streamlined approach that provides supply chain protections without disrupting existing users. *See supra* para. 41. We also disagree with Zhejiang Dahua's argument that we should not adopt such a procedure due to the effect it could have on the value of already-produced equipment; we believe such concerns are outweighed by the potential that the process could prevent serious national-security harm and that particular concerns would be addressed in the event OET and PSHSB do institute a proceeding. *See infra* paras. 45-46.

[179] 47 U.S.C. § 1601(b); *see also EA Security R&O and FNPRM*, 37 FCC Rcd at 13511-13513, paras. 40-43 (discussing the Commission's broad authority to regulate radiofrequency devices in the service of national security goals).

[180] *EA Security R&O and FNPRM,* 37 FCC Rcd at 13609-11, paras. 296-302

[181] *See, e.g.,* Motorola Comments, ET Docket No. 21-232 at 6-8 (rec. Apr. 7, 2023) (urging the FCC to extend marketing and sales restrictions to currently authorized covered equipment). Furthermore, the Heritage Foundation urged the Commission to engage in widespread revocation but "[a]t a minimum" undertake this prospective approach. Heritage Comments at 3-4.

[182] Heritage Comments at 4.

potential limitations on importation and marketing.[183] We direct OET and PSHSB to include in the analysis, and seek comment on, any relevant public interest factors, such as economic and supply chain considerations. This analysis will primarily rely upon the details of the relevant specific determination(s) used to inform a given entry on the Covered List.[184] In the public interest analysis, OET and PSHSB must give particular weight to the fact that the relevant equipment was determined to pose "an unacceptable risk to the national security of the United States or the safety and security of United States persons."[185] After all, as the Supreme Court has noted in another context, "[i]t is obvious and unarguable that no governmental interest is more compelling than the security of the Nation,"[186] and the Commission has a long history of relying on national security determinations to inform its public interest analysis.[187]

46. Nonetheless, in certain instances, OET and PSHSB could conclude that other factors outweigh the national security risks. The most relevant sources of information for these other public interest factors are the given specific determinations, and accompanying analyses or rules, themselves. For example, OET and PSHSB recently sought public input on updating the Covered List to include certain equipment related to connected vehicles pursuant to a Commerce Department determination.[188] In the same rule in which the Commerce Department made its specific determinations regarding "unacceptable risks," the Commerce Department also delayed the effectiveness of its own restrictions, explaining that "determining the scope of the prohibitions required a balancing of the need to address the undue or unacceptable risk posed by foreign adversary involvement in the connected vehicles supply chain with the impact on the public and industry."[189] While such balancing cannot, under the Secure Equipment Act, affect the Commission's updates to the Covered List and prohibition on granting new equipment authorizations to covered equipment,[190] the Commission may consider such countervailing

[183] For example, the public notice could apply to all "Telecommunications equipment produced by Huawei Technologies Company, including telecommunications or video surveillance services provided by such entity or using such equipment" and its affiliates and subsidiaries. *See* FCC Covered List.

[184] 47 U.S.C. § 1601(b)(1). Zhejiang Dahua claims that these rules are arbitrary and capricious because they do not require any showing of specific or actual harm and that, in the case of Dahua, no details of determination exist. *See* Zhejiang Dahua *ex parte* at 2. We find this argument unpersuasive because we do require justification and a process beyond mere "administrative *fiat*." *See infra* paras 45-46.

[185] 47 U.S.C. § 1601(b)(1); *EA Security R&O and FNPRM*, 37 FCC Rcd at 13511-13512, para. 40 (noting that the inclusion of the phrase "public interest" in section 302(a) of the Act provides authority for the Commission to take into account, in its consideration of the public interest, the national defense and the promotion of safety of life and property).

[186] *Haig v. Agee,* 453 U.S. 280, 307 (1981) (quotation marks and citation omitted).

[187] *China Telecom (Americas)*, Order on Revocation and Termination, 36 FCC Rcd 15966 (2011) (revoking the section 214(a) operating authority of China Telecom (Americas) on public interest grounds based on national security and law enforcement risks), *aff'd*, *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2023); *Pacific Networks Corp. and ComNet (USA) LLC*, Order on Revocation and Termination, 37 FCC Rcd 4220 (2022) (revoking the section 214(a) operating authority of Pacific Networks and ComNet on public interest grounds based on national security and law enforcement risks), *aff'd*, *Pacific Networks Corp. and ComNet (USA) LLC v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023).

[188] *The Public Safety and Homeland Security Bureau and the Office of Engineering and Technology Seek Public Input on Commerce Department Determination Regarding Certain Connected Vehicle Technologies,* WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233, Public Notice, DA 25-418 (May 23, 2025) (*Connected Vehicles Public Notice*).

[189] Department of Commerce, Bureau of Industry and Security, *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 90 Fed. Reg. 5360, 5363 (Jan. 16, 2025); *see also id.*, 90 Fed. Reg. at 5377 ("BIS believes that this appropriately balances addressing the national security risks posed by software that is actively maintained in the PRC and Russia while lowering potential burdens and disruptions to the market.").

[190] *See* 47 U.S.C. § 1601(b)(1), (c)(2).

economic concerns when implementing the prohibitions for already-authorized devices outlined in this rule.

47. While the specific determination must be the centerpiece of OET and PSHSB's analysis, they also will fully consider evidence in the Commission's record regarding whether to adopt a limitation on an existing authorization with regard to continued importation or marketing of the equipment. The public notice must provide an opportunity for public comment for a minimum of 30 days and may provide an opportunity for reply comments if OET and PSHSB find it warranted. After the end of the comment period(s), OET and PSHSB will review all relevant information, request additional information if needed, and make their determination as to whether to implement the prohibition on importation and marketing, describing what equipment is subject to the limitation, and providing the reasons for such. So as to promote regulatory certainty and the continued confidence of the public in our efforts to secure the communications equipment supply chain, OET and PSHSB should take reasonable steps to conclude these proceedings expeditiously after the end of the relevant comment period.

48. We direct OET and PSHSB to, as soon as practicable, institute proceedings to determine whether to apply these prohibitions to some or all of the equipment currently on the Covered List. We also direct OET and PSHSB to, simultaneous with any future addition of equipment to the Covered List or as soon as practicable thereafter, issue a Public Notice requesting public comment on whether to apply these prohibitions to such equipment.

49. For any devices for which an existing equipment authorization is limited to prohibit continued importation and marketing (which includes sale[191]), the relevant responsible parties would be obligated to ensure compliance with such prohibition. For equipment certifications, the responsible party is the party to whom the grant of certification is issued, also referred to as the "grantee."[192] As for SDoC authorizations of covered equipment, the responsible party could be the manufacturer, the assembler, the importer, retailers, original equipment manufacturers, or the party performing modifications to the equipment.[193] OET and PSHSB should include in the initial public notice proposed timelines by which the responsible parties must cease all importation and marketing activities and specifically seek comment on such, thereby encouraging dialogue not only with the responsible parties but also with the relevant manufacturers, importers, distributors, retailers, and other interested entities. Such timeline considerations should include, in addition to the underlying national security concerns, factors such as the quantity of devices that have already been imported into the U.S. and are available for or being held for marketing or sale, new or recently updated device models that are *en* route to the U.S. or pending shipment, and devices that are subject to executed distribution, marketing, or sales agreements but have not yet entered the supply chain although they are contemplated for such.

50. We find that this process will help to ensure that OET and PSHSB are fully considering the ramifications of the implementation of the proposed prohibition, not only with regard to the relevant grantee or responsible party, but also the public at large. We are confident that this process will thereby effectuate an outcome that remains consistent with the original specific determination regarding the equipment pursuant to the Secure Networks Act and the Secure Equipment Act while balancing the public interest factors regarding the supply chain and consumer interests. Because this limitation on existing authorizations would not result in the revocation of an existing authorization of covered equipment, the continued use of such equipment that is already in the hands of users would remain authorized. We thereby eliminate several complexities and reduce the challenges that commenters suggested would arise if the only manner to prohibit the importation and marketing of already-authorized covered equipment was to engage in revocations that also prohibit the use or operation of such covered equipment. [194]

[191] 47 CFR § 2.803(a).

[192] 47 CFR § 2.909(a).

[193] 47 CFR § 2.909(b).

[194] *See, e.g.,* Motorola Comments at 6-8.

3. Broad Scope of the Prohibition on Authorization of Equipment Identified on the Covered List

51. *Interpreting whether equipment is "produced by" a specified entity.* To help implement the prohibition on authorization of any covered equipment, applicants seeking equipment certification are required to make certain attestations (in the form of written and signed certifications) about the equipment for which they seek authorization–these include certifying that the equipment is not covered equipment and stating whether the applicant is an entity identified on the Covered List (either a named entity or a subsidiary or affiliate of the named entity).[195] Congress, through the Secure Networks Act, directed the Commission to add to the Covered List equipment defined in 2019 NDAA § 889, all of which is described as "produced by" certain entities: Huawei Technology Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and their affiliates and subsidiaries.[196] Accordingly, for purposes of their attestations, applicants necessarily must determine whether the equipment is "produced by" these entities. Similarly, to ensure that no covered equipment is authorized through the SDoC process, responsible parties that obtain authorizations under SDoC procedures are required to attest that the equipment is not "produced by" any entity identified on the Covered List.[197]

52. FDD notes the potential "ambiguity surrounding the term 'produced by' in the context of covered equipment."[198] FDD expresses concern that the term might not include certain complex forms of foreign adversary control and encourages the Commission to formally adopt a broad definition of the term to ensure that the Commission addresses "instances in which covered vendors serve as original equipment manufacturers or design contractors for companies not listed on the Covered List."[199] The Commission made clear in the *EA Security R&O and FNPRM* that, considering the national security concerns implicated in this proceeding, it was taking a "broad and inclusive" approach to interpreting the scope of what constitutes covered equipment.[200] The Commission also expressed concern regarding authorization of re-branded or re-labeled ("white labeled") covered equipment produced by entities identified on the Covered List, and it made clear that re-branding or "white labeling" of any covered equipment does not change the status of whether the equipment is covered equipment.[201]

---

[195] *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)(C), (3)(i)(C).

[196] This equipment appears as the first five listings on the Covered List–equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua. *See* Covered List, https://www.fcc.gov/supplychain/coveredlist. For example, the first entry on the Covered List is "Telecommunications equipment *produced by* Huawei Technologies Company, including telecommunications or video surveillance services provided by such entity or using such equipment." Covered List (emphasis added).

[197] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13527-28, paras. 82-83; 47 CFR § 2.938(b)(2).

[198] FDD Comment at 4.

[199] FDD Comment at 4.

[200] *See, e.g.*, *EA Security R&O and FNPRM*, 37 FCC Rcd at 13567-68, para. 189 (interpreting the terms of determinations made by the enumerated entities under Secure Networks Act); *id*. at 13568, para. 191 (interpreting the terms "telecommunications" and "video surveillance" equipment broadly to ensure that no covered equipment is authorized); *id*. at 13569-71, para. 194-96 (interpreting "telecommunications" equipment broadly); *id*. at 13571, para. 197 (affirming the Commission's earlier broad approach in implementing the advanced service providers' annual reporting requirement on covered equipment); *id*. at 13573-74, para. 201 (concluding the Congress intended to take a broad view of covered "telecommunications equipment" for purposes of the Commission's prohibition); *id*. at 13576, para. 208 (interpreting "public safety" broadly when discussing prohibition on Hytera, Hikvision, and Dahua covered equipment).

[201] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13567, paras. 187-88.

53. Consistent with the approach in the *EA Security R&O and FNPRM*, when carrying out their responsibilities associated with the prohibition on authorization of covered equipment under section 2.903(a),[202] or any of the required attestations related to covered equipment, applicants, responsible parties, and entities named in their reporting obligations should take a broad view of the term "produced by."[203] This is consistent with Congress's intent to guard against a broad array of equipment through 2019 NDAA § 889 and the Secure Networks Act. Although we decline to adopt a comprehensive definition of "produced by" as FDD suggests, we clarify here that in determining whether a device is "produced by" a particular entity, a broad interpretation likely includes substantial responsibility for or control over any major stage of the process by which a device comes into existence. Accordingly, "produced by" is not limited to the manufacture or assembly of a device. For example, a device would generally be considered to have been "produced by" Huawei if Huawei designed, manufactured, assembled, or developed the device.[204] It is entirely possible that a device would be understood as "produced by" more than one entity. Determining whether a device is produced by a particular entity could be based on multiple factors or the totality of circumstances, particularly when considering the role played by multiple entities to bring a device into existence. We note that this analysis would not necessarily apply to future listings of equipment on the Covered List. Such listings may use different language that indicates an intent to capture a larger or smaller set of communications equipment.[205]

54. *Modification of equipment, including permissive changes.* In the *EA Security R&O and FNPRM*, the Commission adopted revisions to section 2.932 regarding modifications to equipment (*e.g.*, changes in the design, circuitry, or construction of the device) and section 2.1043 concerning changes to certified equipment, such as "permissive changes."[206] The Commission noted that a modification to authorized equipment could result in the later identification of that equipment as covered and determined that it could not allow the continued authorization of modified equipment if, at the time of such modification, the equipment is covered equipment.[207] The Commission adopted requirements, similar to the revised provisions of section 2.911, that all applications or requests to modify already certified equipment include a written and signed certification that the equipment is not prohibited from receiving an equipment authorization pursuant to section 2.903.[208] It also required an affirmative or negative statement as to whether the applicant is identified on the Covered List, as well as the written and signed certifications required under section 2.911(d)(6) regarding an agent for service of process within the

[202] 47 CFR § 2.903(a).

[203] We also note, for instance, the definition and synonyms of the verb "produce" include, among other things, make, manufacture, construct, generate, create, assemble, supply, deliver, or be the source of. *See, e.g.*, *Thesaurus*, https://www.thesaurus.com/browse/produce (last visited Oct. 23, 2025); Merriam Webster, *Produce*, https://www.merriam-webster.com/dictionary/produce (last visited Oct. 23, 2025).

[204] Furthermore, we ordinarily assume that any entity submitting an application for certification or serving as the responsible party for SDoC would be considered among those producing the device. *See also* Horizon Advisory Comments at 4 (noting that Chinese companies often work to "'localize' their production via joint ventures and tie-ups" or "sell into the US market through supply relationships with original equipment manufacturers" or "[t]echnology licensing arrangements.").

[205] *See*, *e.g.*, *Connected Vehicles Public Notice* (referring to equipment "designed, developed, manufactured, or supplied by" certain entities, rather than "produced by"). Eagle Electronics, a U.S. module manufacturer, urges the Commission not to consider a device "produced by" a particular entity "solely due to the originating design IP" if "the device has been substantially altered and secured by an independent U.S. owner." Eagle Electronics *ex parte* at 3. We make no assertion here that our intent is to consider originating design IP as a sole factor in determining whether a device is produced by a particular entity.

[206] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13516, para. 52; 47 CFR §§ 2.932, 2.104.

[207] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13521-22, paras. 65-66.

[208] 47 CFR § 2.1043(b)(2)(i)(B), (b)(3)(i)(B).

United States.[209] The Commission adopted the same provisions for requests for Class II and III permissive changes pursuant to section 2.1043.[210] The Commission found these revisions sufficient to prevent modified equipment from maintaining authorization when such modifications occur at a time after which such equipment has been identified as posing a risk and thereby appearing on the Covered List.

55. We now clarify that 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. This clarification is consistent with Congress's direction to the Commission in the Secure Equipment Act to "clarify that it will no longer review or approve any application for equipment authorization for" covered equipment.[211] Any application for authorization of covered equipment is thereby prohibited under section 2.903, including applications for permissive changes. For permissive changes that do not require an application and thereby are not reviewed by the Commission, the prohibition still applies because such changes are approved by the Commission if they meet the requirements of that type of change as provided in the rules (*i.e.*, they are "approved by rule"). We further modify the rule revisions of sections 2.932 and 2.1043 adopted in the *EA Security R&O and FNPRM* to clarify this prohibition.

4. Benefits and Costs

56. We find the targeted measures of this Report and Order will advance national security objectives in an efficient manner without incurring substantial costs. The measures on the prohibition of modular transmitters and on the broad scope of the prohibition on authorization of equipment produced by entities identified on the Covered List are clarifications of the measures from the *EA Security R&O and FNPRM*. As such, these represent minimal changes that simply ensure realization of the original benefits and costs of the *EA Security R&O and FNPRM*. The measures on limitation of existing authorization of covered equipment will involve additional work in compliance from affected entities. As previously stated, we find that these measures are necessary because obsolescence is insufficient to completely address issues with already authorized covered equipment. However, we do believe that obsolescence will mitigate compliance costs due to the relatively short equipment life cycles. By delegating authority to OET and PSHSB to limit the scope of the marketing and importation prohibition, we are ensuring that any costs to affected entities are specific enough to meet critical national security needs but are still narrow. Moreover, we emphasize that we are currently not requiring manufacturers to replace equipment in the hands of consumers. In doing so, we are tailoring our rules in such a way as to make sure that the public benefits outweigh any costs that our prohibition will impose.

---

[209] 47 CFR § 2.1043(b)(2)(i)(C), (b)(3)(i)(C). In implementing the revisions to section 2.1043, the Commission re-numbered several paragraphs in that section. The Commission has since identified cross-references in other Commission rules that were not updated accordingly. We now adopt the necessary rule revisions to update those cross-references. Section 553 of the Administrative Procedure Act permits us to amend our rules without undergoing notice and comment where we find good cause that doing so is "impracticable, unnecessary, or contrary to the public interest." 5 U.S.C. § 553(b)(3)(B). The Commission has previously determined that notice and comment is not necessary for "editorial changes or corrections of typographical errors." *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Order, 37 FCC Rcd 6865, 6927, para. 156 (2022). Consistent with Commission precedent, in this instance we find that notice and comment is unnecessary for adopting a ministerial revision to section 2.933(b)(5) to correct the misnumbered cross-references.

[210] Class 2 and Class 3 permissive changes are significant enough that they require submission of test results. *See* 47 CFR § 2.1043(b)(2)-(3). Therefore, the requested certification that the equipment is not on the Covered List and an attachment identifying the agent for service of process would be submitted along with the test results. Because no filings are currently requested for the less significant Class 1 permissive changes, *see* 47 CFR § 2.1043(b)(1), this requirement would not apply.

[211] Secure Equipment Act § 2(a)(2).

B. Second Further Notice of Proposed Rulemaking

57. In this Second FNPRM, the Commission aims to further its actions in strengthening our prohibitions on authorization of covered equipment and to clarify the rules and enforcement of such. We seek additional comment on modular transmitters and component parts in relation to covered equipment. We address the partial remand of the Commission's decision in its November 2022 *EA Security R&O*[212] by proposing a definition of "critical infrastructure" as used on the Covered List and seeking comment on the implementation of that definition. We also seek comment on whether any modification to an authorized device by an entity identified on the Covered List should require a new application for certification. Finally, we seek comment on clarifying the scope of activities that constitute marketing of equipment and on measures to strengthen enforcement of marketing prohibitions.

1. Modules and Component Parts

58. In the Second R&O, we clarify that our existing rules prohibiting the authorization of covered equipment include modular transmitters that are on the Covered List.[213] We further prohibit the authorization of any device that includes a modular transmitter identified on the Covered List if the modular transmitter itself would be covered equipment.[214] In this Second FNPRM, we seek further comment on whether the Commission should prohibit authorization of equipment that includes other types of component parts on the grounds that the inclusion of such component parts would render the relevant device covered equipment or on other grounds.

59. In the *EA Security R&O and FNPRM*, the Commission sought comment on other approaches to prohibiting the authorization of covered equipment that focused on component parts at a more granular level, *i.e.*, looking at all of the component parts and considering whether any particular individual component part produced by entities identified on the Covered List potentially raises unacceptable national security risks.[215] In focusing more specifically on the Commission's task of prohibiting authorization of equipment identified on the Covered List, we seek further comment on what other types of components, if installed or included in equipment for which authorization is sought, could lead to the relevant device posing the same unacceptable risk as covered equipment. In other words, what role should particular component parts play in the assessment of whether we should prohibit the authorization of a given device? Commenters should describe component parts they believe to be relevant to our inquiry and explain their view as to how various components, if included in equipment for which authorization is sought, would affect this analysis. Commenters should provide detail regarding the factors that the Commission should consider. For example, should we prohibit authorization of any equipment that contains covered equipment, even if that equipment is not a modular transmitter? Alternatively, should we prohibit authorization of equipment that includes component parts that are logic-bearing hardware, firmware, or software produced by entities identified on the Covered List?[216] Should

---

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

[213] *See supra* paras. 14-**Error! Reference source not found.**

[214] *See id.*

[215] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13604-05, para. 285.

[216] The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (the Committee or Team Telecom) informed the Commission in another proceeding that foreign adversaries can exert influence via companies using "logic-bearing hardware, firmware, or software" designed, produced, or maintained by "high-risk providers identified by the United States government." *See* Team Telecom Comment to *Evolving Risks NPRM* at 6; *see also Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, et al.,* OI Docket No. 24-
(continued….)

we, in other words, prohibit authorization of communications equipment that would be covered equipment as a result of its inclusion of logic-bearing hardware, firmware, or software? Should the Commission expressly prohibit authorization of devices that include semiconductors produced by entities identified on the Covered List, as one commenter recommends,[217] or would semiconductors be included within the definition of "logic-bearing hardware, firmware, or software"? If the Commission were to prohibit authorization of equipment that includes component parts other than modular transmitters on the grounds that their inclusion would lead to the relevant device being classified as covered equipment, we ask that commenters explain how the Commission could identify such components with sufficient specificity for interested parties (including applicants, suppliers, TCBs, and industry) to identify equipment that would be prohibited from authorization. We further seek information on the cost, process, and feasibility of identifying and reporting all component parts included within a device, and any options that could help to reduce the burden of doing so while still meeting the intent to identify covered equipment. We also seek information on the availability of U.S. or non-foreign adversary produced replacements.

60. We underscore that our goal in this proceeding is to ensure that the Commission not authorize equipment that poses an unacceptable risk to national security in accordance with the Covered List specific determinations. We note that several commenters state that they are already participating in other governmental efforts to improve equipment security,[218] and they advocate a "whole of government" approach to address the component parts issues.[219] We believe that those ongoing efforts are critical, but do not fully address the Commission's statutory responsibilities to implement the prohibition on authorization of covered equipment and to promulgate regulations concerning radiofrequency devices consistent with the public interest.[220] We believe that the Commission has the requisite authority to prohibit authorization of equipment that includes certain component parts and seek comment.

61. We seek comment on the appropriate transition period, if any, for implementing a prohibition on the authorization of equipment that includes certain component parts that we seek to identify.[221] The

---

523, MD Docket No. 24-524, Further Notice of Proposed Rulemaking at para. 293 (*Submarine Cable FNPRM*) (proposing to prohibit the use of logic-bearing hardware produced by any entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary). Team Telecom is a source for additions to the Covered List. 47 U.S.C. § 1601(c)(1) (referring to "any executive branch interagency body with appropriate national security expertise"); *see, e.g.*, *Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act,* WC Docket No. 18-89, Public Notice, DA 22-320 at 2 (Mar. 25, 2022). Team Telecom's comment in our proceeding does not qualify as a "specific authorization" for the purposes of our Covered List, but is it suggestive of the types of components that (if produced by entities on the Covered List) would render a device covered, given Team Telecom's role as an enumerated source for Covered list additions and the Commission's long history of deferring to Team Telecom's expertise on national security questions?

[217] *See* Hudson *Ex Parte* at 2.

[218] *See, e.g.*, CTA Comments at 1-3; CTIA Comments at 2-4; USTelecom Comments at 1-3.

[219] *See, e.g.*, ACIL Comments at 8 (supports the Commission working with federal agencies in a whole-of-government approach); CTIA Comments at 4-6,8 (ICT security demands a whole-of-government approach, and national uniformity is critical; the FCC should not attempt to identify ranges of components based on its own assessment, and instead should rely on whole-of-government effort); TIA Comments at 5 (the FCC should rely on a whole-of-government approach, along with consultation with industry). *Cf.* CTA Comments at 8-9 (the FCC should not pursue developing its own standards that may be at odds with the national security agencies).

[220] 47 U.S.C. § 302a(b).

[221] As noted supra, commenters raise potential supply chain concerns and make various recommendations regarding the need for a transition period before a component part prohibition goes into effect. *See, e.g.*, CTIA Comments at 10-11 (the Commission should provide industry with at least two years to find replacement parts); ITI Comments at 7 (the Commission should provide a "reasonable amount of time" to find a replacement module); TIA Reply at 5 (if (continued….)

Commission's prohibition on authorization of covered equipment is based on national security concerns, so the Commission must take those security concerns into account. We ask that commenters address the extent to which a particular transition period is recommended for a particular component part, and explain the rationale and bases for such views. In addition, we seek further comment and quantitative estimates on how different transition period durations (e.g., 6 months, 12 months, or longer) would impact the supply chains for such components and equipment containing such components. As we noted supra, several commenters recommend that the Commission work closely with industry to establish the appropriate transition period if particular component parts are deemed covered equipment,[222] and we invite further comment on this approach.

62. Several commenters express concern about potential supply chain disruptions and about the potential need to ensure the procurement of replacement parts.[223] We seek comment on the specific details and costs of such disruption. We also ask for specific comment on any transition or phase-in prior to the effective date of a prohibition on the authorization of equipment that includes any particular components, and an explanation of the basis for any particular suggested period, including the time necessary for identifying the component part(s) in equipment for which authorization is sought and for obtaining replacements.[224] Commenters advocating for a transition period should provide clear explanations for the factors they believe the Commission should take into consideration, and how the Commission should weigh such factors given the important national security goals that would be furthered by a prohibition on authorization of equipment that includes such components. The Commission requests further comment on the optimal transition path that strikes the appropriate balance between addressing national security concerns in a timely manner and allowing a smooth market transition that minimizes impact on the equipment supply chain.

63. Finally, we also seek comment on one of Charles Parton's proposals in our *EA Security R&O and FNPRM*. Mr. Parton recommends, among other things, that the government "[p]ass legislation or implement administrative measures to prevent the purchase of new Chinese IoT modules for domestic manufacturing and services."[225] We construe this as suggesting the Commission prohibit the authorization of equipment containing certain modular transmitters that are not necessarily produced by entities identified on the Covered List. We seek comment on this suggestion and ways to implement such a prohibition. For example, should we prohibit the authorization of any equipment that contains a modular transmitter produced by any person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as that term is used elsewhere in Commission rules?[226] What national

---

the FCC extends covered equipment to include component parts, the FCC should provide ample time for manufacturers to source, test, and integrate new parts into their products); Competitive Carriers Association Reply at 8 (the FCC should allow a transition period of at least two years); Verizon June 29, 2023 *Ex Parte* at 2 (the FCC should engage in industry consultation to gather information regarding the transition periods necessary to implement any particular component ban; transition period should be sufficient to allow global market to adjust to avoid supply chain shortages).

[222] *See, e.g.*, Verizon June 29, 2023 *Ex Parte* at 2 (the FCC should engage in industry consultation to gather information regarding the transition periods necessary to implement any particular component ban).

[223] *See, e.g.*, ACIL Comments at 6; CTIA Comments at 10-11 (the Commission should provide industry with at least two years to find replacement parts); ITI Comments at 7 (a "reasonable amount of time" should be provided to find a replacement module); TIA Reply at 5 (if the FCC extends covered equipment to include component parts, the FCC should provide ample time for manufacturers to source, test, and integrate new parts into their products); Verizon June 29, 2023 *Ex Parte* at 2 (transition periods should be sufficient to allow global markets to adjust to avoid supply chain shortages); USTelecom Comments at 4-5; Competitive Carriers Association Reply at 6-7; Hikvision Comments at 30-36.

[224] *See*, *e.g.* Eagle Electronics *Ex Parte* at 4.

[225] Charles Parton Report at 2.

[226] *See* 47 CFR § 1.70001(g).

security risks justify such an action? We note that Mr. Parton seems not to be alone in his views, as other national security professionals have indicated that modular transmitters produced by foreign adversaries, like China, pose national security risks.[227] If we were to adopt this proposal, should the Commission exempt modules connected to a foreign adversary entity only by an "historical IP lineage" and manufactured in a secure fashion, as Eagle Electronics recommends?"[228] We seek comment on this perspective.

64. Similarly, the Hudson Institute recommends we prohibit authorization of all equipment that contains a range of components, including semiconductors, modular transmitters, GPS and timing modules, and optical transceivers produced by any person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.[229] We seek comment on this approach. Should the Commission prohibit authorization of equipment that includes these or other such components? We also seek comment on whether we should adopt this list of critical components or a broader or narrower one. How should we identify such components produced by any person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary? What other reason would require, or authorize, the Commission to prohibit equipment authorizations other than by deeming them to be on the Covered List? What, if any, are the national security benefits of such an approach? What are the costs? We seek additional comment on the capabilities of identifying the producer and the resources and analysis required to do so.

65. Finally, we seek comment on other measures proposed in comments in our record. Should we consider any additional measures such as a broader investigation into the security of hardware serving U.S. data centers, to the extent that such hardware is subject to equipment authorization procedures and incudes components that could present risks to national security considerations?[230] Similarly, should the Commission consider developing partnerships with one or more of the enumerated entities that can make "specific determinations" for our Covered List to determine security risks for specific communications equipment or services or developing a trusted supplier program in coordination with federal partners?[231] If so, what information should the FCC consider in development of such a program and what benefits or costs might arise?

2. Critical Infrastructure

66. In this Second Further Notice of Proposed Rulemaking, we address the U.S. Court of Appeals for the District of Columbia Circuit's partial remand of the Commission's decision in its *EA Security*

---

[227] Clete Johnson, *Spies, Saboteurs, and Access to U.S. Connected Devices*, The Liberty Bell Project (July 14, 2025), https://libertybellproject.us/reports/spies-saboteurs-and-access-to-u-s-connected-devices/#mission (raising security concerns about China's dominance in modular transmitters); *see also* Matthew Johnson, *Smart Device Empire, Part 2: Policy Underpins PRC's Global IoT Ambitions*, The Jamestown Foundation (August 7, 2025), https://jamestown.org/program/smart-devices-in-beijings-global-push-for-networked-control/ ("Beijing's expanding control over global IoT supply chains increases its leverage over foreign economies. Its bid for cellular IoT module (CIM) dominance threatens the supply security of rivals, especially amid tensions. … Devices such as drones and connected vehicles equipped with PRC LiDAR or modules can passively map infrastructure for future targeting. … This dominance in IoT hardware has created systemic cybersecurity risks.").

[228] Eagle Electronics *Ex Parte* at 3 (proposing that the criteria for ensuring secure manufacturing include instances where "a U.S. responsible party (1) exercises exclusive design control and exclusive authority over compilation, cryptographic signing, and delivery of firmware/updates for the device's logic-bearing subsystems, (ii) preclude any third-party update pathway through secure-boot/cryptographic binding, and (iii) provides independent security evaluation and supply-chain provenance").

[229] Hudson *Ex Parte* at 1-2.

[230] *Id*. at 2-3.

[231] *Id*. at 3.

R&O and FNPRM.[232] Specifically, the court 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.[233] The court concluded that the guidance was "unjustifiably broad," 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.[234]

67. *2019 NDAA § 889 and the Covered List.* Under 2019 NDAA section 889(f)(3) and the Secure Networks Act, Congress specifically determined that covered equipment includes certain telecommunications and video surveillance equipment produced by five entities—Huawei Technologies Company (Huawei), ZTE Corporate (ZTE), Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), and Dahua Technology Company (Dahua) (and their respective subsidiaries and affiliates).[235] With respect to equipment of the last three of these, Congress listed "video surveillance and telecommunications equipment" produced by these entities only to the extent such equipment is "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[236] In March 2021, consistent with the statutory language of NDAA section 889(f)(3)(B), the Commission included this same language on its Covered List.[237]

68. *Equipment Authorization Security R&O*. In the *EA Security R&O and FNPRM*, the Commission adopted several rules to prohibit authorization of covered equipment.[238] The Commission provided that it would not approve any application for authorization of covered equipment produced by Hikvision, Dahua, Hytera, or their affiliates and subsidiaries that would allow the marketing and selling of this equipment for those particular purposes specified under NDAA section 889(f)(3).[239] The Commission further required that, before the Commission would authorize such equipment, Hikvision, Dahua, Hytera, and their affiliates and subsidiaries must each seek and obtain Commission approval of its respective plan that will ensure that such equipment will not be marketed or sold for any of those purposes.[240] The Commission also provided guidance on the meaning of "for the purpose of public safety,

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

[233] *Hikvision*, 97 F.4th at 948-50. *See* Pub. L. 115-232, § 889, 132 Stat. 1636, 1917-19 (2018) (2019 NDAA § 889); 47 U.S.C. § 1601(c)(3).

[234] *Hikvision*, 97 F.4th at 948-950.

[235] *See* 2019 NDAA § 889(f)(3)(A)-(C); 47 U.S.C. § 1601(c)(3).

[236] 2019 NDAA § 889(f)(3)(B).

[237] *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice, DA 21-309 (Mar. 12, 2021). *See also* Covered List, https://www.fcc.gov/supplychain/coveredlist.

[238] *See supra* paras. 6-7.

[239] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13562, para. 176.

[240] *Id.* at 13564, para. 180.

security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[241]

69. As part of this guidance, the Commission "broadly" construed "critical infrastructure."[242] The Commission cited several sources in the *EA Security R&O and FNPRM,* as supporting its definition of "critical infrastructure." It specifically adopted the meaning provided by the USA PATRIOT Act of 2001 (Patriot Act), which defines "critical infrastructure" as "systems 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 a combination of those matters."[243] But the Commission also relied upon Presidential Policy Directive 21 (PPD-21), which identified 16 critical infrastructure economic sectors,[244] as well as the set of 55 National Critical Functions (NCFs), published by the Cybersecurity and Infrastructure Security Agency (CISA) through the National Risk Management Center (NRMC), to "guide national risk management efforts.[245] The Commission found that for "purposes of implementing the rules" adopted in the *EA Security R&O and FNPRM*, "any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in PPD-21or the 55 NCFs identified in CISA/NRMC could reasonably be considered 'critical infrastructure.'"[246]

70. *Partial Remand of the EA Security R&O and FNPRM.* Hikvision USA and Dahua USA petitioned the court for review of the Commission's *EA Security R&O and FNPRM*.[247] On April 2, 2024, the court issued its decision, denying the petition in part and granting it in part. The court upheld the Commission's decision to prohibit authorization of petitioners' covered equipment and denied petitioners' challenge to the Commission's placement of their equipment on the Covered List.[248] The court, however, granted the petitioners' challenge to the Commission's guidance concerning when equipment is used "for the purpose of . . . physical security surveillance of critical infrastructure."[249]

71. 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

[241] *Id.* at 13576-78, paras. 208-14.

[242] *Id.* at 13576, para. 209.

[243] Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272, 401 (2001) (codified at 42 U.S.C. § 5195c(e)).

[244] 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. In April 2024, PPD-21 was replaced with the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22). *See* 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 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.*; PPD-21 at 10-11.

[245] *See* CISA's "National Critical Functions: An Evolved Lens for Critical Infrastructure Security and Resilience" (Apr. 30, 2019) (National Critical Functions Set), available at https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.

[246] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13577-78, para. 212.

[247] *Hikvision*, 97 F.4th at 940.

[248] *Id.* at 944-50.

[249] *Id.* at 950.

that the Commission adequately explained why the cited sources were relevant."[250] The court specifically found that reliance on these sources "reflects appropriate consideration of relevant factors identifying 'critical' areas of the economy that have been vetted by those in the Executive Branch charged with assessing national security risks."[251] The court, however, noted that the definition of "critical infrastructure" adopted by the Commission includes "any 'systems or assets' that are merely 'connected to' the sixteen sectors identified by PPD-21 or the fifty-five functions listed by the CISA risk management guide." It found that the Commission had failed to explain or justify its use of "the expansive words 'connected to,'" and that the scope of the definition was "therefore arbitrarily broad."[252]

72. The court stated 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.'"[253] 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."[254] 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 had not identified any relevant infrastructure that would not be covered, whether critical or not.[255] The court concluded that the Commission's definition, "[w]ithout further explanation of why its expansive interpretation is reasonable or consistent with the statute," was "not in accordance with law and is arbitrary and capricious."[256] The court also stated that the Commission's decision failed to "provide comprehensible guidance about what falls within the bounds of 'critical infrastructure.'"[257] Finally, it concluded that the Commission had failed to justify placing that burden on petitioners to understand this guidance, and that "without a clear understanding of what constitutes a 'connect[ion] to' critical infrastructure, Petitioners will face significant difficulty in developing" the required "marketing plan"[258] before petitioners' "covered" equipment will be authorized.[259] Thus, the court vacated "the portions of the FCC's order

[250] *Id.* at 949.

[251] *Id.* at 949.

[252] *Id.*.

[253] *Id.* at 949-50.

[254] *Id.* at 950.

[255] *Id.* The "food and agriculture sector" is one of the sixteen "critical infrastructure sectors" identified under PPD-21, and supplying water is associated with another of these sectors, the "water and wastewater systems" sector. The court also noted that the Commission did not rebut petitioners' argument that coffee shops, residential apartment buildings, used car lots, and dry cleaning stores could all plausibly fall with the Commission's definition. We do not read the court's reference to the Commission's failure to rebut the petitioners' arguments as concluding that these entities cannot properly be considered critical infrastructure; rather, as the court opined, under the "connected to" definition of critical infrastructure, "the FCC was unable to identify any relevant infrastructure that would not be covered, whether critical or not." *Hikvision*, 97 F.4th at 950.

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

[257] *Id.* Specifically, the court noted that while the Commission has suggested that petitioners seek guidance from the Commission in the form of a declaratory ruling, it found such a requirement "unworkable." *Id.*

[258] *Id.*

[259] As the court noted, pursuant to the *EA Security R&O and FNPRM*, Hikvision, Dahua, and Hytera telecommunications and video surveillance equipment will not be authorized for sale in the United States until such time as the Commission approves these entities' plans to ensure that such equipment will not be marketed and sold for prohibited purposes. *See Hikvision*, 97 F.4th at 943; *see EA Security R&O and FNPRM*, 37 FCC Rcd at 12561-62, paras. 176-78.

defining 'critical infrastructure'" and remanded to the Commission "to comport its definition and justification for it with the statutory text of the NDAA."[260]

73. *Proposed Definition of Critical Infrastructure*. In this Second FNPRM, we address the D.C. Circuit's partial remand and seek 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. We note that adoption of this definition is a precondition to the review and approval of any compliance plans, as required under the *EA Security R&O and FNPRM*.[261]

74. We propose to define "critical infrastructure" as: "Systems 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 a combination of those matters."[262] This definition would apply the same base definition, taken from the Patriot Act, of "critical infrastructure" that the Commission adopted in the *EA Security R&O and FNPRM*, but exclude the portion that the court found to be arbitrarily broad.[263]

75. We note that this proposed definition has been used several times after its inclusion in the Patriot Act. For instance, both PPD-21 and National Security Memorandum 22 (NSM-22) adopted this definition of "critical infrastructure." We tentatively conclude that the proposed definition is preferable because it is consistent with existing precedent and aligns with current Executive Branch policy directives regarding critical infrastructure.[264] We seek comment on this tentative conclusion. Would another definition of "critical infrastructure" be better? We ask any commenters with reservations about our proposal to provide alternative definitions and explain why those options could be preferable to our proposed definition.

76. We find that this proposal is consistent with the court's opinion, which did not reject a broad definition of "critical infrastructure." 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.[265] 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

[260] *Hikvision*, 97 F.4th at 950. On January 16, 2025, Hikvision USA filed a motion to enforce the court's mandate, in which it: (1) asked the court to require the agency to immediately lift the freeze that prevents it from submitting authorization applications for its equipment, and (2) asked the court to direct the Commission to act "within a set time" on a compliance plan that Hikvision submitted to the Commission. *See* Pet. Hikvision USA, Inc.'s Mot. to Enforce the Mandate, *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024) (Nos. 23-1032, 23-1073). On February 10, 2025, Zhejiang Dahua Technology Company, Ltd, filed a motion for similar relief. *See* Resp. of Zhejiang Dahua Technology Co., Ltd. to Mot. to Enforce the Mandate and Mot. for Affirmative Relief, *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024) (Nos. 23-1032, 23-1073). The Commission filed an opposition, explaining that Hikvision's requested relief goes beyond the court's mandate and that Hikvision has failed to establish a "clear and indisputable right" to relief that would warrant the court issuing a writ of mandamus. *See* Resp't's Opp'n to Hikvision USA, Inc.'s Mot. to Enforce the Mandate at 3, *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024) (Nos. 23-1032, 23-1073). On February 27, 2025, the court denied Hikvision USA and Zhejiang Dahua Technology Company, Ltd.'s motions. *See* Order, *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024) (Nos. 23-1032, 23-1073) (per curiam).

[261] *See EA Security R&O and FNPRM*, 37 FCC Rcd at 13564, para. 180.

[262] 42 U.S.C. § 5195c(e)).

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

[264] *See e.g.,* Exec. Order No. 14305, Restoring American Airspace Sovereignty, 90 Fed. Reg. 24719 (Jun. 6, 2025) (relying on the Patriot Act definition to define critical infrastructure).

[265] *See EA Security R&O and FNPRM*, 37 FCC Rcd at 13576-77, para. 209.

adequately explained why the cited sources were relevant."[266] The court noted that even Hikvision conceded that the Commission's application of the Patriot Act definition of critical infrastructure "may be appropriate."[267] Thus, we believe that continuing to use the Patriot Act definition is the best course and is responsive to the court's opinion. Do commenters agree with our approach of using the Patriot Act definition of "critical infrastructure" but excluding the "connected to" language that the court found to be objectionable in the *Equipment Authorization Security R&O*?

77. We seek comment on whether "systems and assets" is sufficient, or whether we should include additional language to encompass other aspects of communications network infrastructure. For example, CISA's website mentions "assets, systems, and networks."[268] Should we include "networks" and incorporate CISA's language into our proposed definition, and if so, why? Or is it clear, in the context of communications, that "networks" are included within the definition as "assets" or "systems" or both? Are there additional terms that we should include to define the scope of the proposed definition?

78. *Scope and Implementation*. We seek comment on how the Commission should implement the proposed definition of "critical infrastructure." What "systems and assets" should be considered "so vital to the United States" within the meaning of the proposed definition? For example, should we rely on definitions found in the Critical Infrastructure Information Act of 2002 (CII Act),[269] which was enacted to protect shared information with the federal government regarding vulnerabilities and threats to the security of private and state and local government critical infrastructure?[270] The CII Act defines "protected system" as "any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure."[271] Should we rely on definitions found in other statutes, such as "information system" which "means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" and "includes "industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers"?[272] Would relying on these definitions in implementing our base definition address the court's concerns about the scope of the Commission's previous definition?[273]

79. We seek comment on interpreting "critical infrastructure" as encompassing equipment when used in the provision of services or functions in the 16 critical infrastructure sectors ("critical services or functions"). This approach would cover equipment that is not, by itself, "so vital to the United States" to be considered "critical infrastructure," but when used to provide critical services or functions that may be the source of significant network security vulnerabilities. We believe that such an approach is likely necessary to mitigate risks posed by vulnerabilities in network equipment within the critical infrastructure sectors that, if exploited, could produce cascading effects that negatively impact the provision of critical services or functions. Do commenters support this approach? If not, what alternatives would they

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

[267] *Id.* at 949.

[268] CISA, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited Jul. 25, 2025).

[269] Critical Infrastructure Information Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002), renumbered by Pub. L. 115-278, 132 Stat. 4168 (2018) (codified as amended at 6 U.S.C. §§ 671-674).

[270] *See* Congressional Research Service, Homeland Security Act of 2002: Critical Infrastructure Information Act at 12 (2003), https://www.everycrsreport.com/files/20030228_RL31762_8b1b13a081ee124d260ee0d77dd8adcce08ccaf5.pdf.

[271] 6 U.S.C. § 671(5).

[272] 6 U.S.C. § 650(14).

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

suggest? We seek comment on whether additional clarification is necessary. For example, should we incorporate the 55 National Critical Functions to further clarify the scope of the proposed definition?

80. Finally, we seek comment on Hikvision USA's definition of "critical infrastructure" as laid out in its filings with the Commission.[274] In its Compliance Plan, Hikvision USA advocates that critical infrastructure should mean "infrastructure that provides essential services to American society. It includes only such systems and assets—governmental and private—that are 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."[275] Hikvision USA then provides a finite list of 10 systems and assets—across multiple sectors—to define the bounds of critical infrastructure.[276] We tentatively conclude that Hikvision USA's approach—which narrows the scope of the Patriot Act definition—leaves open gaps ripe for exploitation. For example, its list of systems and assets excludes several systems and assets included in the 16 critical infrastructure sectors that, if incapacitated or destroyed, would result in "a debilitating impact on security, national economic security, national public health or safety, or a combination of those matters." These include sectors related to communications, critical manufacturing, emergency services, food and agriculture, and healthcare and public health. We tentatively conclude that such an approach is short-sighted, ignores the vulnerabilities associated with various access points within our communications networks and the interconnected nature of our communications networks, and therefore falls far short of the level of network security Congress intended when it enacted the relevant statutes. Such an approach is contrary to the broad interpretation we find necessary in implementing 2019 NDAA § 889, "given the importance of preventing 'covered' equipment from being made available for prohibited uses that would pose an unacceptable risk to national security or the security of U.S. persons."[277] Do commenters agree with our tentative conclusion, or do commenters believe that Hikvision USA's proposal is more consistent with 2019 NDAA § 889 and the Secure Networks Act?

3. Modifications to Authorized Equipment Produced by an Entity Identified on the Covered List

81. In seeking to ensure consistent application of its prohibition on authorization of covered equipment, the Commission has prohibited the utilization of the SDoC process for authorization of equipment produced by any entity identified on the Covered List.[278] The Commission found that the certification process provides the Commission with the necessary oversight to ensure that we are achieving our goals to prohibit authorization of equipment that poses an unacceptable risk, as required by the Secure Equipment Act, and would help prevent covered equipment from improper authorization through the SDoC process in the first place.

82. As affirmed in the *EA Security R&O and FNPRM*, we believe that requiring use of only one process by entities that have already been determined to produce covered equipment will serve the

[274] *See e.g.,* Emergency Request for Commission Action on Hikvision's Compliance Plan, ET Docket No. 21-232, at 12-13 (filed Dec. 13, 2024), https://www.fcc.gov/ecfs/document/1217141177312/1; 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).

[275] April Compliance Plan, at 7.

[276] *See id*. Hikvision's list includes the following items related to the communications sector: facilities that house Internet service provider networks and Internet service provider traffic exchange points; systems and facilities serving military installations, including telecommunications services, information services, and fiber optic cables; submarine cable systems, including associated cables, landing points, maintenance facilities, and data centers; and satellite systems serving the Department of Defense. *See id.*

[277] *EA R&O and FNPRM*, 37 FCC Rcd at 13576-77, paras. 208-09.

[278] 47 CFR § 2.906(d). Entities "identified on the Covered List" generally includes entities named on the Covered List and such entities' affiliates and subsidiaries.

important goal of ensuring consistent application of the prohibition on authorization of any covered equipment, while also providing for more active Commission oversight. Considering the importance of prohibiting equipment for devices that pose an unacceptable risk to national security, and that the Commission continues to assess and refine its rules and procedures to more effectively identify and prohibit equipment that poses an unacceptable risk to national security, we seek comment on additional action we might take to further strengthen and streamline our efforts to identify covered equipment and ensure it is not authorized.

83. As discussed in the R&O portion of this proceeding, modifications and permissive changes to covered equipment are prohibited under our rules,[279] but such procedures are generally available for other equipment produced by entities identified on the Covered List. In keeping with the intent to require one procedure for all equipment authorization applications made by entities identified on the Covered List, we propose to require the submission of a certification for any equipment for which an entity identified on the Covered List seeks modification or a permissive change. For example, a class II permissive change could encompass software changes or modification to internal circuitry which, depending on the specific change, could result in modifying a device such that it could pose an unacceptable risk to national security. How would such a requirement further our goals in protecting the supply chain? Should the Commission consider a streamlined procedure to facilitate such a requirement, and how would a streamlined procedure further our goals in this proceeding? What potential impacts to the supply chain should the Commission consider and in what ways could such negative impacts be mitigated?

4. Clarification of "Marketing" Activities

84. Given the unacceptable risks to national security posed by the continued importation and marketing of covered equipment, we seek comment on how the Commission can strengthen its efforts to prevent unauthorized marketing, including through clarifications to our rules. We believe that strengthening enforcement against unauthorized marketing would not only assist the Commission's mission under the Secure Equipment Act regarding covered equipment, but also have the added benefit of strengthening enforcement against unauthorized or non-compliant equipment more generally.

85. *Clarifying marketing rules.* "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."[280] Historically, the Commission's enforcement efforts for violations of our marketing rules have primarily focused on manufacturers and retailers. However, in many cases, RF equipment producers are foreign manufacturers or their subsidiaries and affiliates, and enforcement actions against such entities may face delays or be hindered by foreign governments. This is particularly likely for entities identified on the Covered List, which the Commission has found are often protected from being investigated by foreign adversaries. We seek comment on whether revisions to our equipment marketing rules could address these challenges by enabling the Commission to better refocus its enforcement on domestic marketing and related activities in an ever-evolving marketplace. For example, what steps should we take to ensure more accountability among resellers or drop shippers of covered equipment for compliance with our rules barring the marketing of covered equipment? Would such efforts assist the Commission's ability to enforce its Covered List rules or other rules around marketing?

86. What about marketing of devices by entities identified on the Covered List? Under section 302 of the Act, the FCC has broad authority to, "consistent with the public interest, … make reasonable regulations … governing the interference potential of devices … applicable to the manufacture, import, sale, offer for sale, or shipment … and to the use of such devices …."[281] The Commission's rules require authorization of a device before marketing, but once an authorization is granted, marketing activities are

[279] *See supra* paras. 54-55.

[280] 47 CFR § 2.803(a).

[281] 47 U.S.C. § 302a.

not limited to the grantee of that authorization.[282] That is, in general, our rules allow any entity to market an authorized device. We seek comment on whether our rules should continue to allow marketing of an authorized device regardless of the identity of the marketer. If an entity identified on the Covered List is part of the distribution chain for previously authorized devices, then that entity would have some access or control over those devices while in legal or physical possession of them. The Commission believes that there is a risk to the public in the potential for entities identified on the Covered List—which have been determined to present a risk to national security in some circumstances—to manipulate or modify authorized equipment in a way that could result in that equipment posing a risk to national security or causing harmful interference to radio communications. Would it be in the public interest for the Commission to prohibit marketing of RF equipment by entities identified on the Covered List, regardless of the identity of the authorization holder or the production source?[283] For example, some entities are identified on the current Covered List only with regard to the telecommunications services they provide;[284] should the Commission consider a marketing prohibition of authorized devices for such entities? What are the potential impacts to the supply chain, if any? What other concerns should the Commission consider?

87. *Clarifying responsibility for ensuring compliance in the importation process*. Several different types of entities may be involved in the importation process, including a foreign importer of record, a domestic purchaser, an ultimate consignee, or the proprietor of a warehouse that receives goods after their entry or release into the United States. Section 2.1204(b) of the Commission's rules provides that the "ultimate consignee [of an imported RF device] must be able to document compliance with the selected import condition."[285] A consignee may be a commercial intermediary that contracts with a retailer to take delivery of imported goods immediately after entry, or a consignee may be the purchaser of an imported device.[286] Should the Commission clarify who may be held liable for importing unauthorized or noncompliant RF equipment? How might the Commission do so? How would such a clarification benefit the Commission's enforcement ability? Would such an action bring welcome clarity to the Commission's enforcement activities? What costs might be associated with such a clarification?

88. Furthermore, the Commission has previously advised that even online consumers may be engaged in importation when purchased devices are drop-shipped directly to the consumer from overseas.[287] To date, however, the Commission has not focused its enforcement efforts on either consumers or commercial consignees. We tentatively conclude, based on our experience, 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. We seek comment on whether this assessment is correct. We seek comment on which entity should bear greater responsibility for ensuring that only properly authorized devices are imported. We also seek comment on situations in which neither a sale nor a consignment has occurred at the time of importation. In such cases, which domestic party should be held responsible for compliance with the Commission's rules? Commenters should clearly explain their rationale for assigning responsibility to a specific domestic party, with a particular focus on strengthening enforcement of our Covered List rules. Additionally, we seek comment on what measures

[282] *See* 47 CFR § 2.803.

[283] *Supra* para. 53.

[284] *See* Federal Communications Commission, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist (last updated July 23, 2025).

[285] 47 CFR § 2.1204(b).

[286] A consignee may be the "person named in a bill to whom or to whose order the bill promises delivery." *Consignee*, Black's Law Dictionary (12th ed. 2024).

[287] *See The Supply Room, Inc., Oxford, Alabama*, File No.: EB-FIELDSCR-12-00002402, Notice of Apparent Liability for Forfeiture and Order, 28 FCC Rcd 4981, 4984, para. 9. (2013) (finding that any person or entity that purchases a signal jamming device online and has it shipped to the United States from a foreign source is the importer and has violated sections 2.1203 and 2.1204 of the Commission's rules); 47 CFR §§ 2.1203, 2.1204.

could improve transparency of equipment authorizations and revocations for both marketing entities and consumers.

89. *Clarifying "distribution" as part of marketing*. The Commission specifically seeks comment on whether we should clarify the term "distribution for the purpose of selling," as used in the definition of marketing. Which specific activities fall under this category, and how do they differ from, or overlap with, other marketing functions? Could activities such as consignment, warehousing, inventory management, order processing, labeling, packaging, billing, and other fulfillment services, individually or collectively, if performed in connection with transportation of RF equipment,[288] constitute distribution for the purpose of sale? Alternatively, could an entity performing any of the foregoing activities without transporting the RF device be considered to be engaged in the distribution for the purposes of sale? How do such entities currently verify that the products they handle are compliant? Which type of entities are best positioned to verify that RF equipment have valid FCC equipment authorizations? We specifically seek comment on how a definition of "distribution" might affect the various party entities that are not themselves engaged in the trade of RF equipment but participate in the distribution of RF equipment.

5. Strengthening Enforcement of Marketing Prohibitions

90. As discussed, the Commission seeks comment on additional measures to safeguard consumers and communications networks from the risks posed by equipment identified on the Commission's Covered List.[289] We believe that stronger enforcement measures are needed to counterbalance the national security risks associated with covered equipment. Therefore, we seek comment on additional measures that we could adopt to safeguard consumers and communications networks from the risks posed by covered equipment.

91. *Post-revocation marketing of covered equipment*. In the Second R&O, we adopt rules to place prohibitions on continued importation and marketing of previously-authorized devices.[290] We seek comment on how the Commission can best ensure that consumers, retailers, and the general public may be informed of such limitations on marketing or importation, as well as any revocations undertaken pursuant to our section 2.939 rules. What obligations, if any, should the Commission impose on retailers, sellers and re-sellers, e-commerce websites, importers, distributors, or advertisers to ensure that the public is aware of the authorization status of radio frequency equipment? For example, the Commission has certain requirements for displaying a certified device's FCC ID number. Should we require that number to be visible on the outside of all packaging so a consumer, in all cases, can easily verify a device's authorization status? Similarly, should we require on-line retailers to display the FCC ID number in the product listings for all offered RF products that are subject to certification requirements? We seek comment on what actions the Commission should take to ensure that covered equipment is kept out of the marketplace and out of consumers' hands. To ensure only appropriately authorized equipment is marketed, we seek comment on whether the Commission should require periodic verification of the equipment authorization status of imported inventory prior to marketing? Such periodic reviews would provide opportunities for importers, retailers, etc. to verify the equipment status for RF devices in their inventory; *i.e.*, ensure that the authorization status of equipment in their inventory has not changed during the interim period since purchase and entry into the supply chain. If we adopt such a requirement, what interval of verification would be effective in promoting compliance without imposing an undue burden? Commenters should justify their proposed interval and explain why it would be more appropriate or effective than other alternative intervals. What obligations, if any, should we place on entities within the supply chain and in what time frame should such entities be required to inform other constituents, including end users, within their supply chains of any change in status to equipment available for sale or

[288] Section 302(c) of the Act provides that "carriers transporting such devices or home electronic equipment and systems without trading in them" are exempt from the marketing rules. 47 U.S.C. § 302a(c).

[289] *See supra* paras. 57-88.

[290] *See supra* paras. 32-50.

already sold? What, if any, broader measures should the Commission consider to facilitate verification of an equipment authorization? Should the Commission consider implementation of an expiration date or other time limit on equipment authorizations? If so, what would be a reasonable timeframe and what processes should the Commission consider to facilitate such? Should authorization holders be required to resubmit a full application, or would a simplified application process be appropriate for entities with existing authorizations seeking to renew? Do authorization holders have any reliance interests in maintaining their authorization that the Commission should take into account? What are some advantages and disadvantages of such a timeframe beyond authorization verification?

92. *Tools to identify equipment for which authorization has been revoked or limited*. We seek comment on tools or data sources that could help the Commission, consumers, retailers, and other stakeholders identify equipment for which authorization has been revoked or limited to prevent continued marketing within the United States. Considering that trade model names and numbers are easily changed and that devices can be marketed under names different from those identified on the equipment authorization grant, what procedures could the FCC implement that would aid identification of specific devices for which authorization has been revoked or limited? Could an electronic notification system inform registered users when equipment revocations or limitations on future importation or marketing occur? Would a public, collaboratively maintained platform help ensure the list remains current and accessible? Commenters should specifically explain any concerns with these proposed tools and the feasibility in using such methods to identify unauthorized and revoked equipment.

93. *Ongoing compliance practices by marketing entities*. We seek comment on what specific policies, practices, or tools we should implement to stay informed of the current equipment authorization status of devices that they market. What compliance monitoring practices do industry participants currently employ to monitor compliance, and what are the associated costs or burdens with each of those methods? Commenters should be as specific as possible regarding any current best practices providing citations and/or links to such best practices, where applicable. Which of these practices, if any, should the Commission consider incorporating into its rules? Are there tools the Commission could employ to efficiently audit or verify compliance? Commenters should provide specific examples of potential tools to verify compliance. To further assure both retailers and consumers that equipment is authorized for marketing and to facilitate verification that each device has a valid authorization, should the Commission explicitly require display of the FCC ID at the online point of sale or at other virtual points of sale?

6. Benefits and Costs

94. The proposal regarding modular transmitters simply seeks information, while the proposals regarding critical infrastructure and marketing involve clarifications of particular terms. Since these clarifications do not involve a clear change in policy, we have no counterfactual against which to estimate costs or benefits. Rather, we find that they simply help realize the benefits and costs from the *EA Security R&O and FNPRM*. The proposal that requires the submission of a certification for any equipment for which an entity identified on the Covered List seeks modification or a permissive change may result in additional needed actions for compliance. However, we do not expect a substantial increase in associated costs. The number of entities on the Covered List is likely to be low, and they are likely to file fewer equipment authorization applications because some of their equipment will no longer be approved under any process. Overall, we anticipate that the eventual proposal will be a cost-effective faithful execution of Congressional intent to enhance national security but seek information on the benefits and costs of these proposals and any proposed implementation.

IV. PROCEDURAL MATTERS

95. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),[291] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings,

[291] 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).

unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[292] 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.

96. 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.

97. *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. 104-13. 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 107-198, 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."

98. *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.[293] 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 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.

99. *Providing Accountability Through Transparency Act.* Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of this document will be available on https://www.fcc.gov/proposed-rulemakings.

100. *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).

[292] 5 U.S.C. § 605(b).

[293] 47 CFR § 1.1200 *et seq.*

- 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.
    - 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.

101. *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).

102. *Congressional Review Act*. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, 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 Second Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

103. *Availability of Documents.* Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS.

104. *Further Information*. For further information, contact Jamie Coleman of the Office of Engineering and Technology, at 202-418-2705 or Jamie.Coleman@fcc.gov.

V. ORDERING CLAUSE

105. Accordingly, 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, and the Secure Equipment Act of 2021, Pub. L. 117-55, 135 Stat. 423, 47 U.S.C. § 1601 note, that this Second Report and Order and Second Further Notice of Proposed Rulemaking IS HEREBY ADOPTED.[294]

106. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this Second Report and Order and Second 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.

[294] 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).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

For the reasons set forth in the document above, the Federal Communications Commission amends 47 CFR part 2 as follows:

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

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

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

2. Amend § 2.803 by revising the introductory text of paragraph (b) to read as follows:

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

* * * * *

(b) *General rule.* No person may market a radio frequency device unless the radio frequency device is authorized pursuant to a valid FCC equipment authorization that has not been limited through the procedures described in section 2.939(e) of this chapter, and:

* * * * *

3. Amend § 2.903 by:

a. Revising paragraph (a);

b. Redesignating paragraphs (b) through (d) as paragraphs (d) through (f); and

c. Adding new paragraphs (b) and (c).

The revisions and additions read as follows:

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

(a) All equipment on the Covered List, as established pursuant to § 1.50002 of this chapter, is prohibited from obtaining an equipment authorization under this subpart. This includes equipment that:

(1) Has been certified as a modular transmitter; or

(2) Meets the modular transmitter requirements of § 15.212 of this chapter and could be certified as a modular transmitter.

(b) All equipment that incorporates equipment meeting the descriptions in paragraph (a)(1) or (2) of this section is prohibited from obtaining an equipment authorization under this subpart.

(c) The prohibitions in paragraphs (a) and (b) of this section apply to:

(1) Equipment that would otherwise be subject to certification procedures;

(2) Equipment that would otherwise be subject to Supplier's Declaration of Conformity procedures; and

(3) Equipment that would otherwise be exempt from equipment authorization.

* * * * *

4. Amend § 2.932 by revising paragraphs (b) and (c) to read as follows:

§ 2.932 Modification of equipment.

* * * * *

(b) Except for equipment prohibited from authorization pursuant to § 2.903, permissive changes may be made in certificated equipment, and equipment that was authorized under the former type acceptance procedure, pursuant to § 2.1043.

(c) Permissive changes may be made in equipment that was authorized under the former notification procedures unless such equipment meets one of the criteria in paragraphs (1) or (2). The grantee must submit information documenting continued compliance with the pertinent requirements upon request.

(1) The equipment is currently subject to authorization under the certification procedure; or

(2) The equipment is prohibited from authorization pursuant to § 2.903 of this chapter.

* * * * * 5. Amend § 2.933 by revising paragraph (b)(5) to read as follows:

§ 2.933 Change in identification of equipment.

* * * * *

(b) * * *

(5) The photographs required by § 2.1033(b)(10) or (c)(14) showing the exterior appearance of the equipment, including the operating controls available to the user and the identification label. Photographs of the construction, the component placement on the chassis, and the chassis assembly are not required to be submitted unless specifically requested.

* * * * *

6. Amend § 2.939 by:

a. Revising the section heading;

b. Revising paragraph (a) introductory text; and

c. Adding paragraph (e).

The revisions and additions read as follows:

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

(a) The Commission may revoke, or place limitations pursuant to paragraph (e) of this section on, any equipment authorization:

* * * * *

(e) The Office of Engineering and Technology (OET) and the Public Safety and Homeland Security Bureau (PSHSB) may place limitations on an existing authorization for covered equipment authorizations to prohibit continued importation or marketing, pursuant to the following procedures:

(1) OET and PSHSB will issue a public notice announcing the intent to limit the scope of equipment authorizations to prohibit the further importation or marketing of specified devices identified by class, type, or other description sufficient to identify the devices.

(2) The public notice will include an assessment of the impact of the proposed prohibition with consideration of public interest factors, including: the unacceptable risks the equipment was found to pose, the economic and supply chain impacts, and any other criteria as specified by the Commission. The public notice should give particular weight to the specific determination(s), and any accompanying rules or analyses, through which the relevant equipment was added to the Covered List.

(3) The public notice will provide for a public comment period of no less than 30 days.

(4) OET and PSHSB will review the submissions, may request additional information as may be appropriate, and must make their determination as to whether to place limitations on the existing authorization to prohibit the further importation or marketing of the relevant devices, providing the reasons for such decision.

7. Amend § 2.1043 by revising the introductory text of paragraph (b) to read as follows:

§ 2.1043 Changes in certificated equipment.

* * * * *

(b) Except for equipment prohibited from authorization pursuant to § 2.903, three classes of permissive change may be made in certificated equipment without requiring a new application for and grant of certification. Any of these classes of changes must not result in a change in identification.

* * * * *

8. Amend § 2.1204 by revising paragraph (a)(1) to read as follows:

§ 2.1204 Import conditions.

* * * * *

(a) * * *

(1) The radio frequency device is authorized pursuant to a valid FCC equipment authorization that has not been limited through the procedures described in § 2.939(e).

* * * * *

APPENDIX B

Proposed Rules

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

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

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

2. Amend § 2.907 by revising paragraph (c) to read as follows:

§ 2.907 Certification.

* * * * *

(c) Any equipment produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, that would otherwise be eligible for authorization pursuant to the Supplier's Declaration of Conformity, would be exempt from equipment authorization, or for which an authorization was previously granted and a permissive change would otherwise be permitted, must obtain equipment authorization through the certification process.

3. Amend § 2.932 by adding paragraph (f) as follows:

§ 2.932 Modification of 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.

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 *Equipment Authorization Security Report and Order, Order, and Further Notice of Proposed Rulemaking* (*EA Security R&O and FNPRM*).[2] The Commission sought written public comment on the proposals, 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. The Second R&O expands 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 Second R&O, the Commission adopts clarifications and revisions to our part 2 rules. Specifically, we prohibit the authorization of devices that include modular transmitters that are covered equipment and clarify our rules to state that covered equipment includes modular transmitters. Additionally, we clarify the term " produced by" as used on the Covered List and the prohibition on modifications, including permissive changes, to previously authorized covered equipment. Lastly, we adopt a procedure to limit previously granted authorizations of covered equipment, including permissive changes, to prohibit the continued importation and marketing without affecting the continued operation or use of such equipment. 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.

---

[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*; *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*). The instant Second R&O and Second FNPRM only addresses issues in ET Docket No. 21-232 concerning matters relating to the Commission's equipment authorization program and does not address matters relating to the Commission's competitive bidding program raised in EA Docket No. 21-233.

[3] 5 U.S.C. § 604.

[4] *See EA Security R&O and FNPRM*.

[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.

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

4. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA,[6] the Commission is required to respond to any comments filed by the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy, and provide a detailed statement of any change made to the proposed rules as a result of those comments.[7] 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 proposed rules, if adopted.[8] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[9] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act (SBA).[10] 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.[11] 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.[12]

6. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[13] In general, a small business is an independent business having fewer than 500 employees.[14] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[15] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant their field.[16] 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

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

[7] 5 U.S.C. § 604 (a)(3).

[8] 5 U.S.C. § 603(b)(3).

[9] *Id*. § 601(6).

[10] *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."

[11] 15 U.S.C. § 632.

[12] 13 CFR § 121.903.

[13] 5 U.S.C. § 601(3)-(6).

[14] *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.

[15] *Id*.

[16] 5 U.S.C. § 601(4).

employees.[17] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[18] 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.[19]

7. The rules adopted in the Second R&O will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[20] codes and corresponding SBA size standard.[21] Based on currently available U.S. Census data regarding the estimated number of small firms in each identified industry, we conclude that the adopted rules will impact a substantial number of small entities. Where available, we provide additional information regarding the number of potentially affected entities in the above identified industries.

Regulated Industry (NAICS Classification)	**NAICS Code**	**SBA Size Standard**	**Total Firms**[22]	**Small Firms**[23]	**% Small Firms in Industry**
Other Communications Equipment Manufacturing[24]	334290	750 employees	321	310	96.57
Radio Stations[25]	516110	$47 million	2,963	1,879	63.42
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing[26]	334220	1,250 employees	656	624	95.12
Satellite Telecommunications[27]	517410	$47 million	275	242	88.00
Wired Telecommunications	517111	1,500 employees	3,054	2,964	97.05

[17] *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/.

[18] 5 U.S.C. § 601(5).

[19] *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.

[20] 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.

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

[22] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, and *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM.

[23] *Id.*

[24] Affected Entities in this industry include Vendors of Infrastructure Development Network Buildout.

[25] Affected Entities in this industry include Auxiliary, Special Broadcast and Other Program Distribution Services.

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

[27] Affected Entities in this industry include Fixed Satellite Small Transmit/Receive Earth Stations and Mobile Satellite Earth Stations.

Regulated Industry (NAICS Classification)	NAICS Code	SBA Size Standard	Total Firms[22]	Small Firms[23]	% Small Firms in Industry
Carriers[28]					
Wireless Telecommunications Carriers (except Satellite)[29]	517112	1,500 employees	2,893	2,837	98.06
All Other Telecommunications[30]	517810	$40 million	1,079	1,039	96.29

2024 Universal Service Monitoring Report Telecommunications Service Provider Data[31] (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	Total # FCC Form 499A Filers	Small Firms	% Small Entities
Wired Telecommunications Carriers[32]	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)[33]	585	498	85.13

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.[34]

9. In the Second R&O, the Commission's part 2 rules concerning the EA program's requirements, processes, and guidance 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 produced by an entity 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 modular transmitters produced by entities identified on the Covered List, prohibition on importation and marketing, and those posing unacceptable risks to

[28] Affected Entities in this industry include Facilities-Based Carriers (International Telecom Carriers) and Providers of International Telecommunications Transmission Facilities.

[29] Affected Entities in this industry include Fixed Microwave Services, Private Land Mobile Radio Licensees (PLMR) and Radio Frequency Equipment Manufacturers (RF Manufacturers).

[30] Affected Entities in this industry include Internet Service Providers (Non-Broadband), Non Licensee Owners of Towers and Other Infrastructure, and Telecommunications Relay Service (TRS) Providers.

[31] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

[32] Local Resellers fall into another U.S. Census Bureau industry (Telecommunications Resellers) and therefore data for these providers is not included in this industry.

[33] Affected Entities in this industry include all reporting wireless carriers and service providers.

[34] *Id*. § 604(a)(5).

national security. The Commission expects that all filing, recordkeeping, and reporting requirements associated with the adopted rules will be the same for small and other entities.

10. In addition, the revised rules provide for limitations of equipment authorization of any equipment that fails to comply with our rules regarding covered equipment. Consistent with its existing rules in section 2.939(a), concerning the revocation or withdrawal of equipment authorization, the Commission authorizes the Office of Engineering and Technology (OET) and the Public Safety and Homeland Security Bureau (PSHSB) to, if they find cause, provide written notice to the grantee that a revocation proceeding is being initiated and the grounds under consideration for such revocation. Grantees have 10 days to address an initiating revocation proceeding in writing. OET and PSHSB will then review their submission to make their determination as to whether to revoke the authorization or may request additional information, if appropriate.

11. With regard to existing equipment authorizations of covered equipment, OET and PSHSB may limit the scope to prohibit continued importation or marketing of any authorized equipment. The bureaus must provide notice of the intent to limit the scope of an equipment authorization(s) to prohibit the further importation or marketing of specified devices. The notice must include an assessment of the impact of the proposed prohibition with consideration of public interest factors and allow no less than 30 days for public comment prior to a definitive decision.

12. The Commission expects that the actions taken in the Second R&O 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 modular transmitters and the broad scope of the prohibition on authorization of equipment produced by entities 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. In addition, while we cannot conclusively determine whether the rules adopted in the Second R&O 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.

13. With the adoption of the Second R&O, 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

14. 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."[35]

15. The Second R&O 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 modular transmitters in devices. Other expert agencies determined that the equipment included on the Covered List poses an unacceptable risk to national security. Pursuant to Executive Order 12866, the FCC considered alternatives to this rule that would impose less of a societal burden. The FCC did not

[35] *Id*. § 604(a)(6).

find any reasonable alternative that would have decreased the impact on small entities but still achieve the objective of the rule.

16. Through its review of the record in this proceeding and in its ultimate adoption of the rules set forth in the Second R&O, 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. We considered an approach favoring sweeping revocations that would require small and other entities to implement a widespread revocation of existing authorizations of equipment subsequently identified on the Covered List. Such an approach would require the removal and replacement of equipment already in use. Instead, the adopted rules reduce excessive burdens on small and other entities by providing a simplified and prospective approach in which previously granted authorizations of covered equipment are limited to prohibiting the continued importation and marketing of such equipment, without limiting their continued operation or use.

17. In addition, the Second R&O concerning section 2.939's revisions, giving a grantee of covered equipment 10 days to respond to the Commission's initiating revocation proceeding reflect a reasonable and cost-effective method that ensures equipment authorizations are prohibited from further importation or marketing of specified devices. We believe that most grantees, some of which are small entities, will rely on boilerplate language that, once incorporated for a single written response, will be of negligible cost to include in future written responses. Moreover, we note that the previous attestation requirement adopted in the *EA Security R&O and FNPRM*,[36] is more cost effective to small and other entities than an alternative approach, such as a verification process in which a third party would confirm that the equipment being certified is not on the Covered List since that type of third party verification would be substantially more costly to applicants and would likely slow innovation. We believe that the costs we are imposing are reasonable in light of the national security goals.

18. Similarly, we find that the existing requirement that agents or service of process on behalf of authorization grantees are located within the United States is both reasonable and cost effective. This will substantially reduce the cost to grantees by avoiding our enforced prohibition on importation and marketing of equipment on the Covered List.

G. Report to Congress

19. The Commission will send a copy of the Second R&O, including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act.[37] In addition, the Commission will send a copy of the Second R&O, including this Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the SBA and will publish a copy of the Second R&O, and this Final Regulatory Flexibility Analysis (or summaries thereof) in the Federal Register.[38]

---

[36] *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 Competitive Bidding Program*, ET Docket No. 21-232, FCC 22-84, 37 FCC Rcd 13493 (15) (EA Security R&O and FNPRM).

[37] 5 U.S.C. § 801(a)(1)(A).

[38] *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 Second Further Notice of Proposed Rulemaking (Second FNPRM) 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 Second FNPRM. The Commission will send a copy of the Second FNPRM, including this IRFA, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.[2] In addition, the Second FNPRM and IRFA (or summaries thereof) will be published in the Federal Register.[3]

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

2. In November 2022, as a means of furthering the Commission's national security objectives of protecting the security of America's communications networks and equipment supply chains, we adopted rules that prohibited and clarified authorization of modular transmitters produced by entities on the Covered List under our existing rules.[4] Furthermore, the *EA Security R&O and FNPRM*),[5] sought comment on complicated approaches on component parts and critical infrastructure defined and provided by the USA PATRIOT Act of 2001 (Patriot Act).[6] The Commission received several recommendations from commenters to establish an appropriate transition period if component parts are deemed covered equipment. Additionally, the *Partial Remand of the Equipment Authorization Security R&O,* granted the petitioners' challenge of the Commission's guidance concerning when equipment is used "for the purpose of . . . physical security surveillance of critical infrastructure."[7]

3. In the Second FNPRM, the Commission addresses the court's remand regarding clarification issues and several other matters which require further comment to promulgate concise rules. Those issues include modular transmitters and component parts in relation to covered equipment, device modifications made by an entity identified on the Covered List, activities that constitute marketing of equipment, and measures to strengthen enforcement against unauthorized marketing. Lastly, we propose alternative definitions of "critical infrastructure" as used on the Covered List. We believe that further comments and proposals would be particularly useful for fine tuning how to identify covered equipment, clarify unauthorized equipment identified as covered equipment from further marketing, and provide comprehensible guidance about what falls within the bounds of critical infrastructure.

---

[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] *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*).

[5] *EA Security R&O and FNPRM*, 37 FCC Rcd at 13576.

[6] Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272, 401 (2001) (codified at 42 U.S.C. § 5195c(e)).

[7] *Hikvision*, 97 F.4th at 948-50.

B. Legal Basis

4. 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

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 proposed rules, if adopted.[8] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[9] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act (SBA).[10] 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.[11] 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.[12]

6. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[13] In general, a small business is an independent business having fewer than 500 employees.[14] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[15] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant their field.[16] 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.[17] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[18]

---

[8] 5 U.S.C. § 603(b)(3).

[9] *Id*. § 601(6).

[10] *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."

[11] 15 U.S.C. § 632.

[12] 13 CFR § 121.903.

[13] 5 U.S.C. § 601(3)-(6).

[14] *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.

[15] *Id*.

[16] 5 U.S.C. § 601(4).

[17] *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/.

[18] 5 U.S.C. § 601(5).

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.[19]

7. The proposals in the Second FNPRM would apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[20] codes and corresponding SBA size standard.[21] Based on currently available U.S. Census data regarding the estimated number of small firms in each identified industry, we conclude that the proposed rules would impact a substantial number of small entities. Where available, we also provide additional information regarding the number of potentially affected entities in the above identified industries.

Regulated Industry (NAICS Classification)	**NAICS Code**	**SBA Size Standard**	**Total Firms**[22]	**Small Firms**[23]	**% Small Firms in Industry**
Electronic Computer Manufacturing	334111	1,500 employees	300	291	97.00
Other Communications Equipment Manufacturing[24]	334290	750 employees	321	310	96.57
Radio Stations[25]	516110	$47 million	2,963	1,879	63.42
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing[26]	334220	1,250 employees	656	624	95.12
Satellite Telecommunications[27]	517410	$47 million	275	242	88.00
Wired Telecommunications Carriers[28]	517111	1,500 employees	3,054	2,964	97.05
Wireless Telecommunications	517112	1,500 employees	2,893	2,837	98.06

[19] *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.

[20] 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.

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

[22] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, and *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM.

[23] *Id.*

[24] Affected Entities in this industry include Vendors of Infrastructure Development Network Buildout.

[25] Affected Entities in this industry include Auxiliary, Special Broadcast and Other Program Distribution Services.

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

[27] Affected Entities in this industry include Fixed Satellite Small Transmit/Receive Earth Stations and Mobile Satellite Earth Stations., and Fixed Satellite Very Small Aperture Terminal (VSAT) Systems.

[28] Affected Entities in this industry include Facilities-Based Carriers (International Telecom Carriers) and Providers of International Telecommunications Transmission Facilities.

Regulated Industry (NAICS Classification)	NAICS Code	SBA Size Standard	Total Firms[22]	Small Firms[23]	% Small Firms in Industry
Carriers (except Satellite)[29]					
All Other Telecommunications[30]	517810	$40 million	1,079	1,039	96.29

2024 Universal Service Monitoring Report Telecommunications Service Provider Data[31] (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	Total # FCC Form 499A Filers	Small Firms	% Small Entities
Wired Telecommunications Carriers[32]	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)[33]	585	498	85.13

D. 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 requirements and the type of professional skills necessary for preparation of the report or record.[34]

9. The Second FNPRM 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 Second FNPRM may create additional reporting, recordkeeping, and other compliance requirements for small entities. For example, if the Commission were to adopt rules that identify other component parts that should be prohibited from their use in equipment, the duration of the transition period ultimately adopted for implementing such a prohibition could potentially impact recordkeeping and other compliance requirements for small entities. Further, requiring the submission of a certification for any equipment for which an entity identified on the Covered List seeks modification or a permissive change would also potentially create additional compliance requirements for small entities.

[29] Affected Entities in this industry include Fixed Microwave Services, Private Land Mobile Radio Licensees (PLMR), Radio Frequency Equipment Manufacturers (RF Manufacturers) and Wireless Carriers and Service Providers.

[30] Affected Entities in this industry include Internet Service Providers (Non-Broadband), Non Licensee Owners of Towers and Other Infrastructure, and Telecommunications Relay Service (TRS) Providers.

[31] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

[32] Local Resellers fall into another U.S. Census Bureau industry (Telecommunications Resellers) and therefore data for these providers is not included in this industry.

[33] Affected Entities in this industry include all reporting wireless carriers and service providers.

[34] 5 U.S.C. § 603(b)(4).

10. The Second FNPRM seeks comment on information from interested parties, and clarification of specific terms, regarding how covered equipment is identified. As a result, the Commission is not currently in a position to determine the economic impact of reporting, recordkeeping, or other compliance requirements on small entities. 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 request comments specific to any potential burdens or costs to small entities 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

11. 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.[35] 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 rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[36]

12. As discussed above, the *EA Security R&O and FNPRM* sought comment on how best to strengthen our prohibitions on 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 Second FNPRM's request for additional comment. In formulating its request for comments in the Second FNPRM, the Commission considered alternatives addressing the economic impact of its proposals on small entities, should they be adopted. For example, depending on its requirements, a proposed rule that clarifies the definition of "critical infrastructure" as used on the Covered List could potentially disrupt equipment supply chains for small and other entities, and could lead to additional costs for such entities. We seek comment on ways to find an appropriate balance between addressing national security concerns in a timely manner while allowing a smooth market transition that minimizes impact on the equipment supply chain. Additionally, any proposed rules that impose obligations on an entity within the supply chain to inform other constituents within their supply chains of any change in equipment authorization status to equipment available for sale or already sold could create economic hardship on the reporting entity. By seeking additional comment an considering other approaches, the Commission could clarify the scope of activities that constitute the marketing of equipment and measures to strengthen the enforcement of marketing prohibitions.

13. The Commission will fully consider the economic impact on small entities as it evaluates the comments filed in response to the Second FNPRM, 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

14. None.

[35] *Id.* § 603(c).

[36] *Id.* § 603(c)(1)-(4).

STATEMENT OF
CHAIRMAN BRENDAN CARR

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Second Report and Order and Second Further Notice of Proposed Rulemaking, ET Docket No. 21-232 (October 28, 2025).

The Commission has a long history of working together on a bipartisan basis to protect our networks from insecure gear. In fact, it was over 7 years ago now that I first proposed that the agency consider ordering the removal of untrustworthy equipment and prohibiting this spy gear from entering our networks in the first place.

Since then, multiple Administrations, Congresses, and FCCs have come together and taken action. The FCC prohibited Huawei, ZTE, and similar bad actors from obtaining federal subsidies. The FCC revoked the authority of entities that would do the CCP's bidding, like China Unicom and China Telecom, from connecting to our networks. The FCC has overseen the removal of insecure gear from our networks. The FCC has banned Covered List entities from selling new models of their relevant gear. And we recently prohibited Bad Labs, including those located in China, from participating in our equipment authorization program.

These have all been good and important steps towards securing our communications networks. But America's foreign adversaries are constantly looking for ways to exploit any vulnerabilities in our system.

For instance, we have known for years that devices produced by Huawei, Hikvision, and other Covered List entities threaten America's national security. But up to now, FCC rules have not prevented Covered List providers from continuing to sell previously authorized device models. Nor have those rules applied to a device's component parts. These present loopholes that bad actors could use to threaten the security of our networks.

So we take action on both fronts today.

First, we adopt rules that will allow the FCC to prohibit the importation, marketing, or sale of previously authorized devices on a case-by-case basis. With this new rule, the FCC will have a targeted process it can use to address threats posed by the ongoing sales of devices manufactured by Covered List entities.

Second, we adopt rules that will close the component parts loophole. Specifically, these new rules will allow the FCC to prohibit, not only a finished or completed device produced by a Covered List entity, but also otherwise compliant devices that include certain component parts produced by those bad actors.

Finally, the Commission also seeks comment today on a range of ideas that would further enable the agency to crack down on devices that threaten America's national security.

For their work on the item, I want to thank to Deborah Broderson, Rebecca Clinton, Jamie Coleman, Doug Klein, Shannon Lipp, Neal McNeil, Siobahn Philemon, Kevin Pittman, Chris Smeenk, and George Tannahill.

STATEMENT OF
COMMISSIONER OLIVIA TRUSTY

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Second Report and Order and Second Further Notice of Proposed Rulemaking, ET Docket No. 21-232 (October 28, 2025).

Protecting the integrity of our nation's communications networks is a matter of national security. The actions we take today strengthen our commitment to the integrity of our networks by ensuring that equipment and components posing unacceptable risks to the United States are not authorized, marketed, or deployed in our communication systems.

With this Second Report and Order, we close potential loopholes in our equipment authorization process. We make clear that our rules apply not just to complete devices, but also to modular transmitters and components that can serve as the building blocks of our networks. We also establish a clear process to prevent the continued importation and marketing of equipment that has already been authorized but is later identified as a security threat. These steps are essential to maintaining the trustworthiness of our supply chain and the reliability of our networks.

Our rules must evolve as technology evolves. As communications equipment becomes increasingly modular and globally sourced, national security risks can arise at any point in the supply chain. By clarifying key definitions, such as "produced by," and prohibiting modifications that could reintroduce covered equipment into the marketplace, we are staying ahead of those risks and reinforcing the integrity of our authorization framework.

I also welcome the Second Further Notice of Proposed Rulemaking, which seeks input on additional safeguards, including the treatment of component parts, a clear definition of "critical infrastructure," and stronger enforcement tools. These are forward-looking measures that will help ensure our rules remain both rigorous and adaptable.

Protecting our communications networks is a collective responsibility, one that spans agencies, industries, and borders. I am grateful to the staff of the Office of Engineering and Technology for their technical rigor and to our interagency partners for their collaboration and vigilance. With this item, the Commission once again affirms that when it comes to national security, we cannot afford complacency. The integrity of our networks, and the trust of the American people, depend on it.