FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 2

[ET Docket No. 21-232; FCC 25-71; FR ID 318981]

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

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission or FCC) aims to further its actions in strengthening prohibitions on authorization of covered equipment and to clarify the rules and enforcement of such. The Commission seeks additional comment on modular transmitters and component parts in relation to covered equipment. The Commission addresses the partial court remand of the decision in its November 2022 EA Security R&O by proposing a definition of "critical infrastructure" as used on the Covered List and seeking comment on the implementation of that definition. The Commission also seeks 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, the Commission seeks comment on clarifying the scope of activities that constitute marketing of equipment and on measures to strengthen enforcement of marketing prohibitions.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by ET Docket No. 21-232, by any of the following methods:

- *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.

- *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.

FOR FURTHER INFORMATION CONTACT: Jamie Coleman of the Office of Engineering and Technology, at Jamie.Coleman@fcc.gov or 202-418-2705.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Second Further Notice of Proposed Rulemaking (*Second FNPRM*), in ET Docket No. 21-232, FCC 25-71, adopted on October 28, 2025, and released on October 29, 2025. The full text of this document is available for public inspection and can be downloaded at https://docs.fcc.gov/public/attachments/FCC-25-71A1.pdf. Alternative formats are available for people with disabilities (Braille, large print, electronic files, audio format) by sending an email to *fcc504@fcc.gov* or calling the Commission's Consumer and Governmental Affairs Bureau at (202) 418–0530 (voice), (202) 418–0432 (TTY).

Regulatory Flexibility Act. The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice-and-comment rulemaking, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities." Accordingly, the Commission has prepared an Initial Regulatory

Flexibility Analysis (IRFA) concerning the possible impact of the rule and policy changes contained in the *Second FNPRM* on small entities. The IRFA is set forth in Appendix D of the Report and Order and Further Notice of Proposed Rulemaking.

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, will be inviting 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), the Commission will seek specific comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

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

Synopsis

Introduction

In November 2022, as part of the Commission's 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, ET Docket No. 21-232 and EA Docket 21-233 (2022) (EA Security R&O and FNPRM). 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. 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 the equipment authorization program to protect our nation's communications networks and

supply chains. Building on the record received, Commission experience implementing the prohibition, and other recent Commission actions aimed at protecting our nation's communications networks and supply chain, the Commission adopted a Second Report and Order (Second R&O) and this Second Further Notice of Proposed Rulemaking (*Second FNPRM*) to take important next steps in modifying the equipment authorization program.

Background

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). In June 2021, the Commission initiated this proceeding in 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 (2021) (EA Security NPRM). 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.

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. In particular, the Commission adopted several revisions to its 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 Communications Act. 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).

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. Commission 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. 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. 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). 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, and that none of these grants are for covered equipment. 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. 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.

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 and it did not revoke previously granted authorizations of covered equipment. The Commission determined that both of these matters, along with several other issues, would receive further consideration.

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. 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. 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, as well as the extent to which it should take into account supply chain considerations. 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. 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.

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. *Hikvision USA, Inc. v. Federal Communications Commission*, 97 F.4th 938 (D.C. Cir. 2024). On April 2, 2024, the court issued a partial remand concerning one part of the Commission's decision. 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). 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.

In May 2025, the Commission adopted Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program, ET Docket No. 24-136, 40 FCC Rcd 3616 (2025) (EA Integrity R&O and FNPRM), in which it 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. 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 the Commission's equipment authorization program, including both the equipment certification process and SDoC process. 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. 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. In addition, it also clarified that Commission 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 the equipment authorization program. 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 lists from federal agencies or statutes. 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. Finally, it sought further comment on post-market surveillance procedures to ensure compliance relating to prohibitions on authorization of covered equipment.

Further Notice of Proposed Rulemaking

In this *Second FNPRM*, the Commission aims to further its actions in strengthening its prohibitions on authorization of covered equipment and to clarify the rules and enforcement of such. The Commission seeks additional comment on modular transmitters and component parts in relation to covered equipment. The Commission addresses the partial remand of the decision in its November 2022 EA Security R&O by proposing a definition of "critical infrastructure" as used on the Covered List and seeking comment on the implementation of that definition. It also seeks 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, the Commission seeks comment on clarifying the scope of activities that constitute marketing of equipment and on measures to strengthen enforcement of marketing prohibitions.

A. Modules and Component Parts

In the Second R&O, the Commission clarifies that the existing rules prohibiting the authorization of covered equipment include modular transmitters that are on the Covered List. The Commission further prohibits the authorization of any device that includes a modular transmitter identified on the Covered List if the modular transmitter itself would be covered equipment. In this *Second FNPRM*, the Commission seeks further comment on whether it 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.

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. In focusing more specifically on the Commission's task of prohibiting authorization of equipment identified on the Covered List, the Commission seeks 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 the Commission should prohibit the authorization of a given device? Commenters should describe component parts they believe to be relevant to the 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 the Commission prohibit authorization of any equipment that contains covered equipment, even if that equipment is not a modular transmitter? Alternatively, should the Commission prohibit authorization of equipment that includes component parts that are logic-bearing hardware, firmware, or software produced by entities identified on the Covered List? Should the Commission, 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, 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, the Commission asks 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. The Commission further seeks 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. The Commission also seeks information on the availability of U.S. or non-foreign adversary produced replacements.

The Commission underscores that its 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. The Commission notes that several commenters state that they are already participating in other governmental efforts to improve equipment security, and they advocate a "whole of government" approach to address the component parts issues. The Commission believes 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. 47 U.S.C. 302a(b). The Commission believes that it has the requisite authority to prohibit authorization of equipment that includes certain component parts and seeks comment.

The Commission seeks comment on the appropriate transition period, if any, for implementing a prohibition on the authorization of equipment that includes certain component parts that it seeks to identify. The Commission's prohibition on authorization of covered equipment is based on national security concerns, so the Commission must take those security concerns into account. The Commission asks 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, the Commission seeks 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. Several commenters recommend that the Commission work closely with industry to establish the appropriate transition period if particular component parts are deemed covered equipment, and the Commission invites further comment on this approach.

Several commenters express concern about potential supply chain disruptions and about the potential need to ensure the procurement of replacement parts. The Commission seeks comment on the specific details and costs of such disruption. The Commission also asks 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. 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.

Finally, the Commission also seeks comment on one of Charles Parton's proposals in the 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." The Commission construes 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. The Commission seeks comment on this suggestion and ways to implement such a prohibition. For example, should the Commission 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? *See* 47 CFR 1.70001(g). What national security risks justify such an action? The Commission notes 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. If the Commission 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?" The Commission seeks comment on this perspective.

Similarly, the Hudson Institute recommends the Commission 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. The Commission seeks comment on this approach. Should the Commission prohibit authorization of equipment that includes these or other such components? The Commission also seeks comment on whether it should adopt this list of critical components or a broader or narrower one. How should the Commission 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? The Commission seeks additional comment on the capabilities of identifying the producer and the resources and analysis required to do so.

Finally, the Commission seeks comment on other measures proposed in comments in the record. Should the Commission 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? Similarly, should the Commission consider developing partnerships with one or more of the enumerated entities that can make "specific determinations" for the Covered List to determine security risks for specific communications equipment or services or developing a trusted supplier program in coordination with federal partners? If so, what information should the FCC consider in development of such a program and what benefits or costs might arise?

B. Critical Infrastructure

In this Second Further Notice of Proposed Rulemaking, the Commission addresses the U.S. Court of Appeals for the District of Columbia Circuit's partial remand of the Commission's decision in its EA Security R&O and FNPRM. 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. *Hikvision USA, Inc. v. Federal Communications Commission*, 97 F.4th 938 (D.C. Cir. 2024). 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.

2019 NDAA section 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). 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." 2019 NDAA section 889(f)(3)(B). 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.

Equipment Authorization Security R&O. In the EA Security R&O and FNPRM, the Commission adopted several rules to prohibit authorization of covered equipment. 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). 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. The Commission also provided guidance on the meaning of "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."

As part of this guidance, the Commission "broadly" construed "critical infrastructure." 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." 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)). But the Commission also relied upon Presidential Policy Directive 21 (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), which identified 16 critical infrastructure economic sectors, 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. 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.'"

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. 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. 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."

The court concluded that "[t]he Commission's choice of reference materials—government sources that define 'critical infrastructure' and related national security concepts—was reasonable, and that the Commission adequately explained why the cited sources were relevant." 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." 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."

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.'" 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." 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. 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." The court also stated that the Commission's decision failed to "provide comprehensible guidance about what falls within the bounds of 'critical infrastructure.'" 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" before petitioners' "covered" equipment will be authorized. Thus, the court vacated "the portions of the FCC's order defining 'critical infrastructure'" and remanded to the Commission "to comport its definition and justification for it with the statutory text of the NDAA."

Proposed Definition of Critical Infrastructure. In this *Second FNPRM*, the Commission addresses the D.C. Circuit's partial remand and seeks comment on establishing a new definition of "critical infrastructure" for purposes of the prohibition on authorization of covered equipment produced by Hikvision, Dahua, and Hytera, and their subsidiaries and affiliates. The Commission notes 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.

The Commission proposes 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." 42 U.S.C. 5195c(e)). 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.

The Commission notes 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." The Commission tentatively concludes that the proposed definition is preferable because it is consistent with existing precedent and aligns with current Executive Branch policy directives regarding critical infrastructure. The Commission seeks comment on this tentative conclusion. Would another definition of "critical infrastructure" be better? The Commission asks any commenters with reservations about this proposal to provide alternative definitions and explain why those options could be preferable to the proposed definition.

The Commission finds 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 section 889 as having broad scope with respect to Hikvision, Dahua, and Hytera equipment because such equipment poses an unacceptable risk to national security. The court concluded that "[t]he Commission's choice of reference materials—government sources that define 'critical infrastructure' and related national security concepts—was reasonable, and that the Commission adequately explained why the cited sources were relevant." The court noted that even Hikvision conceded that the Commission's application of the Patriot Act definition of critical infrastructure "may be appropriate." Thus, the Commission believes that continuing to use the Patriot Act definition is the best course and is responsive to the court's opinion. Do commenters agree with the 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?

The Commission seeks comment on whether "systems and assets" is sufficient, or whether it should include additional language to encompass other aspects of communications network infrastructure. For example, CISA's website mentions "assets, systems, and networks." Should the Commission include "networks" and incorporate CISA's language into the 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 the Commission should include to define the scope of

the proposed definition?

Scope and Implementation. The Commission seeks comment on how it 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 the Commission rely on definitions found in the 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) (CII Act), 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? 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." 6 U.S.C. 671(5). Should the Commission 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"? 6 U.S.C. 650(14). Would relying on these definitions in implementing the base definition address the court's concerns about the scope of the Commission's previous definition?

The Commission seeks 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. The Commission believes 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 suggest? The Commission seeks comment on whether additional clarification is necessary. For example, should the Commission incorporate the 55 National Critical Functions to further clarify the scope of the proposed definition?

Finally, the Commission seeks comment on Hikvision USA's definition of "critical infrastructure" as laid out in its filings with the Commission. 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." Hikvision USA then provides a finite list of 10 systems and assets—across multiple sectors—to define the bounds of critical infrastructure. The Commission tentatively concludes 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. The Commission tentatively concludes that such an approach is short-sighted, ignores the vulnerabilities associated with various access points within communications networks and the interconnected nature of 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 the Commission finds necessary in implementing 2019 NDAA section 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." Do commenters agree with this tentative conclusion, or do commenters believe that Hikvision USA's proposal is more consistent with 2019 NDAA section 889 and the Secure Networks Act?

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

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. 47 CFR 2.906(d). The Commission found that the certification process provides the Commission with the necessary oversight to ensure that it

is achieving its 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.

As affirmed in the *EA Security R&O and FNPRM*, the Commission believes that requiring use of only one process by entities that have already been determined to produce covered equipment will serve the 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, the Commission seeks comment on additional action it might take to further strengthen and streamline efforts to identify covered equipment and ensure it is not authorized.

As discussed in the R&O portion of this proceeding, modifications and permissive changes to covered equipment are prohibited under Commission rules, 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, the Commission proposes 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 the Commission's 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 its 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?

D. Clarification of "Marketing" Activities

Given the unacceptable risks to national security posed by the continued importation and marketing of covered equipment, the Commission seeks comment on how it can strengthen its efforts to

prevent unauthorized marketing, including through clarifications to the rules. The Commission believes 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.

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." 47 CFR 2.803(a). Historically, the Commission's enforcement efforts for violations of the 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. The Commission seeks comment on whether revisions to the 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 the Commission take to ensure more accountability among resellers or drop shippers of covered equipment for compliance with its 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?

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 …." 47 U.S.C. 302a. The Commission's rules require authorization of a device before marketing, but once an authorization is granted, marketing activities are not limited to the grantee of that authorization. That is, in general, Commission rules allow any entity to market an authorized device. The Commission seeks comment on whether its 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? For example, some entities are identified on the current Covered List only with regard to the telecommunications services they provide; 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?

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." 47 CFR 2.1204(b). 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. 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?

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. To date, however, the Commission has not focused its enforcement efforts on either consumers or commercial consignees. The Commission tentatively concludes, based on 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. The Commission seeks comment on whether this assessment is correct. The Commission seeks comment on which entity should bear greater

responsibility for ensuring that only properly authorized devices are imported. It also seeks 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 the Covered List rules. Additionally, the Commission seeks comment on what measures could improve transparency of equipment authorizations and revocations for both marketing entities and consumers.

Clarifying "distribution" as part of marketing. The Commission specifically seeks comment on whether to 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, constitute distribution for the purpose of sale? 47 U.S.C. 302a(c). 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? The Commission specifically seeks 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.

E. Strengthening Enforcement of Marketing Prohibitions

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. The Commission believes that stronger enforcement measures are needed to counterbalance the national security risks associated with covered equipment. Therefore, the Commission seeks comment on additional measures that it could adopt to safeguard consumers and communications networks from the risks posed by covered equipment.

Post-revocation marketing of covered equipment. In the Second R&O, the Commission adopts

rules to place prohibitions on continued importation and marketing of previously-authorized devices. The Commission seeks 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 § 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 the Commission 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 the Commission 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? The Commission seeks 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, the Commission seeks 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 the Commission adopts 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 the Commission 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 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?

Tools to identify equipment for which authorization has been revoked or limited. The Commission seeks 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.

Ongoing compliance practices by marketing entities. The Commission seeks comment on what specific policies, practices, or tools it 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?

Ordering Clauses

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 Further Notice of Proposed Rulemaking IS HEREBY ADOPTED.

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

List of Subjects in 47 CFR Part 2

Administrative practice and procedures, Communications, Communications equipment, Reporting and recordkeeping requirements, Telecommunications, and Wiretapping and electronic surveillance.

Federal Communications Commission.

Marlene Dortch,

Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 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 § 2.907 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.

[FR Doc. 2025-21928 Filed: 12/3/2025 8:45 am; Publication Date: 12/4/2025]