PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 26-635
Released: June 26, 2026

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU AND OFFICE OF ENGINEERING AND TECHNOLOGY PROHIBIT THE IMPORTATION AND MARKETING OF PREVIOUSLY AUTHORIZED COVERED COMMUNICATIONS EQUIPMENT ADDED TO THE COVERED LIST IN 2024 OR EARLIER

PS Docket No. 26-72

Introduction

By this Public Notice, the Public Safety and Homeland Security Bureau (PSHSB) and Office of Engineering and Technology (OET) of the Federal Communications Commission (FCC or Commission) prohibit the continued importation and marketing of certain previously authorized covered equipment added to the Covered List in 2024 or earlier.[1] All such covered equipment has been publicly identified as posing "unacceptable risks to the national security of the United States or the security and safety of United States persons"[2] for years. While importation and marketing will be prohibited, this prohibition will not affect the continued use or operation of already-purchased communications equipment. The prohibition adopted in this Public Notice also will not affect equipment added to the Covered List in 2025 or 2026, such as certain foreign-produced Uncrewed Aircraft Systems (UAS), UAS critical components, and routers.[3]

[1] 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 specified sources 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 (FCC Covered List). The process by which the Commission would exercise this authority was established in the *Equipment Authorization Security Second Report and Order*. *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, 40 FCC Rcd 8430, paras. 40-50 (2025) (*EA Security 2d R&O*), *pet. for review pending*, *Hikvision USA, Inc. v. FCC*, No. 25-1274 (D.C. Cir. filed Dec. 3, 2025); 47 CFR § 2.939(e).

[2] 47 U.S.C. § 1601(b).

[3] *See Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List*, WC Docket 18-89, Public Notice, DA 25-1086 (Dec 22, 2025); *FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List*, WC Docket No. 18-89, Public Notice, DA 26-278 (Mar. 23, 2026).

Background

In November 2022, the Commission adopted rules to prohibit authorization of equipment identified on the Covered List.[4] However, the Commission did not revoke previously granted authorizations of covered equipment.[5] In October 2025, the Commission adopted the *EA Security Second R&O* which, among other things, established 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.[6] The Commission noted that its goal was to mitigate potential national security risks associated with covered equipment in the nation's supply chain that was authorized prior to a Covered List addition under 47 U.S.C. § 1601(b).[7] The Commission directed PSHSB and OET to "institute proceedings to determine whether to apply these prohibitions to some or all of the equipment currently on the Covered List" and it delegated authority to PSHSB and OET to apply such prohibitions pursuant to the framework and process outlined in the *EA Security Second R&O*.[8]

The Commission specifically directed PSHSB and OET to conduct a public interest analysis pursuant to that framework, giving "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."[9] Under the framework, PSHSB and OET must first issue a Public Notice with "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."[10] The Public Notice must "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 potential limitations on importation and marketing."[11] The Public Notice must provide "an opportunity for public comment for a minimum of 30 days and may provide an opportunity for reply comments," and PSHSB and OET should take reasonable steps to conclude the proceeding expeditiously.[12]

On March 27, 2026, PSHSB and OET released a Public Notice (March 27 Public Notice) seeking comment on whether the Commission should prohibit the continued importation and marketing of certain previously authorized covered equipment and the relevant factors, including national security and economic and supply chain considerations, that would justify such a prohibition.[13] We tentatively

---

[4] *See generally 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*, Report and Order, Order, and FNPRM, 37 FCC Rcd 13493, 13509-98, paras. 32-263 (2022) (*EA Security R&O and FNPRM*). The Commission 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 chains. *Id.* at 13494-95, para. 1; *see also id.* at 13497-505, 13507-08, paras. 5-23, 31.

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

[6] *EA Security 2d R&O*, FCC 25-71, paras. 40-50; 47 CFR 2.939(e), 2.803, 2.1204.

[7] *Id.* at paras. 32, 40.

[8] *Id.* at paras. 45, 48.

[9] *Id*.

[10] *Id*. at para. 45.

[11] *Id*.

[12] *Id.* at para 47.

[13] *Public Safety and Homeland Security Bureau and Office of Engineering and Technology Seek Comment on Prohibiting the Importation and Marketing of Previously Authorized Covered Communications Equipment Added to the Covered List in 2024 or Earlier*, PS Docket No. 26-72, DA 26-294 (PSHSB/OET Mar. 27, 2026), 91 FR 17275 (Apr. 6, 2026) (*March 27 Public Notice*).

concluded that "prohibiting the importation and marketing of previously authorized covered equipment that was added to the Covered List in 2024 or earlier is consistent with the public interest, because it protects American communications networks from devices specifically determined by Congress or a national security agency to 'pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.'"[14] And we further tentatively concluded that "there are no public interest factors that outweigh our tentative conclusion regarding the proposed ban on import and marketing of this previously [authorized] equipment."[15]

Discussion

Today, based on the record, we prohibit the continued importation and marketing of any covered equipment added to the Covered List in 2024 or earlier. This prohibition specifically applies to all such covered equipment that received FCC equipment authorization before the adoption of our 2022 rules and takes effect 10 days after publication in the Federal Register. As explained further below, however, the prohibition is temporarily suspended for certain equipment added to the Covered List on March 12, 2021, when used for the purpose of physical security surveillance of critical infrastructure, until the Commission adopts a definition of "critical infrastructure." And the prohibition does not apply to any equipment added to the Covered List after 2024. The Commission updated the Covered List webpage to identify the covered equipment that is subject to the prohibition on importation and marketing, which is available at: https://www.fcc.gov/supplychain/coveredlist#importation-marketing-prohibitions.

National security impacts. Protecting national security remains one of the Commission's primary objectives, and the focus of our analysis in this proceeding.[16] Moreover, as the Commission stated in the *EA Security Second R&O*, "no governmental interest is more compelling than the security of the Nation."[17] Consistent with our tentative conclusions in the March 27 Public Notice, we find that prohibiting the continued importation and marketing of previously authorized equipment added to the Covered List in 2024 or earlier is necessary to mitigate national security risks to the U.S. communications sector. In determining whether to adopt such prohibition, the Commission directed that PSHSB and OET "must give particular weight" to the national security determinations made concerning the targeted equipment.[18] The 2021 additions to the Covered List were pursuant to a specific national security determination made by Congress, which the Commission previously found constituted a specific determination that such equipment poses an "unacceptable risk to the national security of the United States or the security and safety of United States persons."[19] Separately, the 2024 addition of "equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software" was based on a specific determination by the Department of Commerce that "Kaspersky's provision of cybersecurity and anti-virus software to U.S. persons, including through third-party entities that integrate Kaspersky cybersecurity or anti-virus software into commercial hardware or software, poses undue and unacceptable risks to U.S. national security and to the security and safety of U.S. persons."[20]

[14] *March 27 Public Notice* at 4-5.

[15] *Id*. at 5.

[16] *EA Security 2d R&O*, FCC 25-71, para. 45; *March 27 Public Notice* at 3.

[17] *EA Security 2d R&O*, FCC 25-71, para. 45 (quoting *Haig v. Agee*, 453 U.S. 280, 307 (1981)).

[18] *EA Security 2d R&O*, para. 45.

[19] 47 U.S.C. § 1601(c)(3); *see also 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, 14315-14316 (2020).

[20] Department of Commerce, Final Determination, Case No. ICTS-2021-002, Kaspersky Lab, Inc., 89 Fed. Reg. 52434 (June 24, 2024), https://www.federalregister.gov/documents/2024/06/24/2024- 13532/final-determination-case-no-icts-2021-002-kaspersky-lab-inc. This action was taken pursuant to Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*. *See* Exec. Order No. 13873, 84 Fed. Reg. 11578 (May 15, 2019).

We agree with CTIA that our action today will "help to mitigate clear national security risks . . . because all of the entities captured in the proposed restrictions have been found by Congress or national security agencies to be subject to the control, direction, or influence of foreign adversary countries."[21]

After review of the record filed in response to the March 27 Public Notice, we reaffirm the Commission's previous finding that older models of covered equipment—many of which remain widely available in the U.S.—continue to pose an unacceptable risk to national security when imported or marketed in the United States, not only when newly introduced to the market.[22] We agree with the Foundation for Defense of Democracies (FDD) that equipment added to the Covered List in 2024 or earlier "is often functionally identical to these firms' more recently banned products" that have been deemed to pose an unacceptable national security risk.[23] We agree as well with FDD that authorized equipment produced by the entities subject to our prohibition "may still be sold in the United States despite the firms" that produce or provide such equipment "continuing to engage in troubling patterns of behavior," including cyberespionage.[24] As FDD states, "[a]llowing them to sell and market previously authorized equipment to the American market will perpetuate vulnerabilities in U.S. telecommunications infrastructure."[25] FDD argues that we "must act to prevent adversaries from exploiting regulatory loopholes to maintain access to U.S. critical infrastructure."[26] Accordingly, we conclude that prohibiting the continued importation and marketing of previously authorized equipment added in 2024 or earlier serves the public interest and is necessary to protect national security by mitigating risks to the U.S. communications sector. No commenter disputed the national security concerns associated with such equipment.

After careful consideration of the record, we also find that arguments concerning economic and supply chain harms do not overcome the preexisting national security determinations and the national security risks posed by the continued importation and marketing of previously authorized covered equipment subject to our action today. We disagree with commenters who argue that the Commission should refrain from extending the prohibition to previously authorized covered equipment because doing so may impose economic costs.[27] We recognize that some parties may face added compliance obligations and lost sales revenue, but those concerns do not override the Commission's responsibility to protect national security. The commenters opposing expansion of the prohibition largely focus on the financial impacts, especially on particular entities.[28] However, these commenters do not meaningfully address the broader consequences of continuing to import and market devices that have been determined to pose

[21] CTIA Comments at 4.

[22] *EA Security 2d R&O*, para. 40.

[23] Foundation for Defense of Democracies Comments at 3 (FDD).

[24] *See* FDD Comments at 1-3; CTIA Comments at 4.

[25] FDD Comments at 3; *see also* USTelecom Comments at 2 (supporting "the Commission's goal of preventing additional deployment of equipment that has been determined to pose national security risks").

[26] FDD Comments at 4.

[27] *See e.g.*, Michael Edwards Comments (filed on behalf of Group One Northwest, Inc.) (there were a total of 22 commenters who used the same template which made similar arguments); *see also* Shane Nevins Comments ; MAXSYSTEMS LA Comments; Accurate Home Audio Inc. Comments; Devlogic Technologies Inc. Comments; Lowe Voltage Pro Comments.

[28] *See, e.g.*, Russell Electric & Security Services Comments (reporting $28,000 in current Hikvision inventory and stating that Hikvision accounts for 100% of its annual revenue); All Around Distributors Comments (reporting $200,000 in current Hikvision inventory and stating that Hikvision accounts for 20% of its annual revenue); Tony Loun Comments (reporting $500,000 in current Hikvision inventory and stating that Hikvision accounts for 30% of its annual revenue).

"unacceptable risks" or provide data for us to consider on those issues, as we invited in the March 27 Public Notice.[29]

As CTIA notes, "the universe of equipment targeted by the [March 27 Public Notice] . . . is produced by a handful of entities," and "[i]n the period since this equipment was added to the Covered List, experience has demonstrated the availability of alternatives."[30] Moreover, devices added to the Covered List as part of the Kaspersky listing in 2024 are already prohibited from importation or marketing under Department of Commerce's rules[31] and equipment added to the Covered List in the initial 2021 listing has not received authorization since November 11, 2022, over three years ago. Thus, we conclude that the national security considerations outweigh the economic and supply chain concerns that commenters raised in the record.

Scope of prohibition for certain equipment. Some of the equipment on the Covered List that was added in 2024 or earlier is "covered" for all uses and purposes.[32] However, as we noted in the March 27 Public Notice, certain equipment added to the Covered List on March 12, 2021, is only on the Covered List when used for specific purposes—namely, "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[33] Under the approach the Commission adopted in the *EA Security R&O*,[34] new equipment authorization applications for covered equipment produced by entities subject to use-based restrictions (i.e., equipment that is covered when "used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes"[35]) are generally prohibited until those manufacturers have submitted, and received Commission approval for, compliance plans.[36] The Commission has yet to approve any such compliance plans, because the Commission's definition of critical infrastructure was the subject of litigation. In 2024, the United States Court of Appeals for the D.C. Circuit upheld the Commission's Order, except for the Commission's definition of "critical infrastructure," which it vacated and remanded back to the Commission to adopt a new definition and justification that "comport[s] . . . with the statutory text."[37] In 2025, in order to address this partial remand of the *EA Security R&O*, the Commission sought comment on a proposed definition of critical

[29] *See March 27 Public Notice* at 4; *see also EA Security 2d R&O* at para. 49.

[30] CTIA Comments at 5; *see also* USTelecom Comments at 5 (the Commission should carefully consider the current state of telecommunications supply chains and the availability of trusted alternatives).

[31] *See* Final Determination at 52437.

[32] *See* FCC Covered List.

[33] *See* FCC Covered List; 2019 NDAA, 132 Stat. at 1918.

[34] *EA Security R&O*, para. 42.

[35] *See* FCC Covered List; 2019 NDAA, 132 Stat. at 1918.

[36] In the *EA Security R&O*, the Commission provided that, consistent with the Secure Equipment Act and the Secure Networks Act, it would not approve any application for authorization of certain covered equipment that would allow the marketing and selling of such equipment to the extent such equipment is "used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." *See EA Security R&O and FNPRM*, 37 FCC Rcd at 13562, para. 176. The Commission further required that, before the Commission would authorize such equipment, entities (and their subsidiaries and affiliates) producing such equipment 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. *Id.* at 13564, para. 180. The Commission further 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." *Id.* at 13576-78, paras. 208-14.

[37] *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 950 (D.C. Cir. 2024).

infrastructure and noted 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*."[38]

Given this backdrop, for any equipment that is "covered" when used for certain purposes, the prohibitions on continued importation and marketing that we adopt today will not apply to importation and marketing for non-"covered" uses. Therefore, the importation and marketing prohibitions will apply *only* to equipment "used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[39] We find that, as urged by two commenters,[40] permitting the importation or marketing of such already-authorized equipment is consistent with the Covered List, the Secure and Trusted Communications Networks Act of 2019, and the Secure Equipment Act of 2021 (Secure Equipment Act).[41] Furthermore, because the Commission currently lacks a definition of, and guidance for interpreting the statutory term "critical infrastructure," we suspend the prohibition on the importation or marketing of such equipment for the purpose of physical security surveillance of critical infrastructure until the Commission adopts such definition and guidance. On the effective date of any Commission Order adopting a definition of "critical infrastructure," importation and marketing will be prohibited for the purpose of "security surveillance of critical infrastructure." Therefore, the importation and marketing of already-authorized equipment subject only to a use-based Covered List entry will only be prohibited if imported or marketed for the purpose of the following, as interpreted in the *EA Security 2d R&O*:

- Public safety;[42]
- Government facilities;[43]
- (Suspended, pending finalized definition of, and guidance for interpreting, "critical infrastructure") physical surveillance of critical infrastructure; and
- "Other national security purposes."[44]

---

[38] *EA Security 2d R&O*, para. 73.

[39] *See* FCC Covered List; John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, 132 Stat. 1636 at 1918 (2018) (2019 NDAA).

[40] *See* Hytera (HCC) Comments at 7-8; Hikvision Comments at 22-23.

[41] *See* Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 (Statutory Notes and Related Subsidiaries) (Secure Equipment Act); Secure Networks Act.

[42] "[T]his includes services provided by State or local government entities, or services by non-governmental agencies authorized by a governmental entity if their primary mission is the provision of services, that protect the safety of life, health, and property, including but not limited to police, fire, and emergency medical services." *EA Security 2d R&O*, para. 210.

[43] As we noted in the *EA Security 2d R&O*, we follow the Cybersecurity and Infrastructure Security Agency's (CISA) description of the "government facilities sector." *See EA Security 2d R&O*, para. 211 ("According to CISA, the government facilities sector includes 'a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments.' In addition to facilities that are open to the public, CISA notes that others 'are not open to the public [and] contain highly sensitive information, materials, processes, and equipment,' and that these facilities include and are not limited to 'general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions.' CISA also notes that '[i]n addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.' We believe that this description provides ample guidance for purposes of what constitutes 'government facilities' for implementation of the prohibition that we adopt today.").

[44] "[W]e interpret this term broadly as encompassing a variety of high-profile assets involving government, commercial, and military assets. In this connection, we note that section 709(6) of the Intelligence Authorization Act (continued….)

Finally, if at any point there is a new specific determination that removes the use-based limits on a Covered List entry, we retain the authority to issue another Public Notice expanding this prohibition to include the importation and marketing of that covered equipment for *all* purposes.

Legal Authority. Without reopening the issue of the Commission's legal authority, we nonetheless note our continued disagreement with Hikvision's arguments that we lack the statutory authority to impose prohibitions on the continued importation and marketing of already-authorized covered equipment.[45] The Commission has previously made clear and explained at length that it has multiple sources of legal authority to limit existing authorizations of equipment that would no longer be eligible to receive authorizations today due to unacceptable national security risks.[46]

We also reject Hikvision's argument that the March 27 Public Notice fails to provide specific notice of affected authorizations under section 2.939.[47] The March 27 Public Notice sufficiently identifies the devices targeted for potential limitation with specific reference to covered equipment that was added to the Covered List in 2024 or earlier.[48] The Covered List clearly reflects the specific equipment that was added to the Covered List, and the date such equipment was added.[49]

Finally, Hytera-US, Inc. (Hytera-US) and Hytera Communications Corporation Limited (HCC) contend that their land mobile radio and digital mobile radio equipment is not "video surveillance and telecommunications equipment," and therefore, in their view, is not covered equipment.[50] As such, they argue that before taking any further action, the Commission must clarify that any restrictions on importing and marketing do not apply to equipment that is not covered equipment.[51] In addition, Hytera-US argues the Commission must lift its hold on Hytera-US's applications for equipment authorizations.[52] HCC similarly argues that the Commission should proceed with a different procedural mechanism than the framework adopted by the Commission in the *EA Security 2d R&O*, so that authorization holders have the ability to contest whether their equipment is subject to the Covered List prohibitions.[53] These arguments do not address the proposals in the March 27 Public Notice, and therefore, we reject these arguments as unresponsive.

Implementation

Existing authorizations. As the Commission has stated, the prohibition on continued importation and marketing does not affect the continued use or operation of previously authorized covered equipment; consumers may continue to use any device or equipment that they currently possess, if the equipment was

for Fiscal Year 2001, provides that 'national security' means the national defense or foreign relations of the United States.' Accordingly, we will rely on this definition for guidance." *EA Security 2d R&O*, para. 213

[45] Hikvision Comments at 1-12.

[46] *E.g.*, *EA Security 2d R&O*, paras. 33 & n.123, 41-42 & n.178; *EA Security R&O and FNPRM*, paras. 32-43, 107, 114-118; *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Notice of Proposed Rulemaking and Notice of Inquiry, ET Docket No. 21-232, 36 FCC Rcd 10578, paras. 65-69 (2021) (*EA Security NPRM*); *see also* Brief for Respondents at 31-51, *Hikvision USA, Inc. v. FCC*, No. 25-1274 (D.C. Cir.).

[47] Hikvision Comments at 24.

[48] *See EA Security 2d R&O*, para. 45.

[49] *See* https://www.fcc.gov/supplychain/coveredlist.

[50] *See* Hytera-US, Inc. Comments at 6 (Hytera-US Comments); HCC Comments at 6-7.

[51] *See* Hytera-US, Inc. Comments at 6.

[52] *See* Hytera-US Comments at 5-6; HCC Comments at 6-7.

[53] *See* HCC Comments at 11.

legally purchased and maintains an existing equipment authorization.[54] Commenters support this approach and no commenter opposed this approach, which is consistent with the *EA Security 2d R&O*.[55] We also note that the importation and marketing prohibitions do not apply to marketing activities that are excepted under statute and the Commission's rules[56] or for importation under the conditions listed in section 2.1204(a)(3)-(11) of the Commission's rules.[57]

Implementation timeline. The prohibition on importation and marketing will take effect 10 days after publication in the Federal Register. As of that date, entities will be prohibited from importing or marketing any covered equipment added to the Covered List in 2024 or earlier. While this approach differs from our proposal in the March 27 Public Notice, which would have required entities to cease all importation and marketing activities within 30 days of the release of this Public Notice, we believe that 10 days following Federal Register publication will create more notice to the public and federal partners. The need for expedited action is especially acute, because a delayed, but looming, prohibition would encourage importers and marketers to flood the U.S. market with covered equipment—a prospect that this proceeding is premised on preventing.

We agree with CTIA that "several factors significantly mitigate any potential supply chain or economic impacts" that may occur as a result of this action, "including previous efforts under the Commission's 'Rip and Replace' program and the long period of time since any equipment produced by the relevant entities has been eligible to be authorized."[58] As CTIA notes, several alternatives have been brought to market since this equipment was added to the Covered List and "participants in the ICT ecosystem can effectively serve the U.S. market without this equipment in their networks or these producers in their supply chains."[59]

We disagree with commenters like NCTA and USTelecom who contend (without specific data to support their arguments)[60] that we should adopt longer and more flexible transition periods to account for supply chain considerations, in-transit equipment, existing inventory, and contractual obligations and reject calls for a "phased implementation."[61] We also disagree with HCC's suggestion that we should broadly exempt from the prohibition "equipment that is used for spare parts, updates and replacements" for existing devices or otherwise "provide a process for reimbursement . . . to allow users to replace the affected equipment."[62] Allowing imports and marketing replacements for existing covered equipment would defeat the entire purpose of this prohibition. As we concluded above, the national security risks of allowing covered equipment to continue to be imported and marketed in the U.S. far outweigh the

[54] *EA Security 2d R&O*, para. 40.

[55] *See* NCTA Comments at 2; USTelecom at 2.

[56] 47 U.S.C. § 302a(c); 47 CFR § 2.807(d) (clarifying that marketing prohibitions do not apply to devices marketed "for use by the Government of the United States or any agency thereof").

[57] 47 CFR § 2.1204(a)(3)-(11).

[58] CTIA Comments at 5.

[59] CTIA Comments at 5.

[60] *See March 27 Public Notice* at 4 (inviting "commenters to provide data that we should consider in our analysis"); *EA Security 2d R&O* at para. 49 (allowing us to consider "the quantity of devices that have already been imported into the U.S. 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," in determining whether to adopt an extended implementation timeline).

[61] *See* NCTA Comments at 5-6; USTelecom Comments at 3.

[62] HCC Comments at 9-10.

potential economic impacts and supply chain disruptions that may occur as a result of this prohibition, and the national security demand for urgent action to avoid flooding the market outweighs any disruption.

Finally, we defer consideration of CTIA's suggestions regarding how to weigh future proceedings placing limitations on the importation or marketing of existing authorizations.[63]

[63] *See* CTIA Comments at 2-3, 6-11.