Federal Communications Commission

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

47 CFR Parts 1, 2, and 15
[ET Docket No. 21-232; FCC 26-50; FR ID 360965]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Washington, DC
August 7, 2026

Introduction

In the case of refining the equipment authorization process, the Federal Communications Commission (FCC) has rounded third, but it hasn't touched home plate yet.

While the FCC has been proactive in protecting the United States from the threats posed by equipment produced by entities on the commission's Covered List, these firms maintain a presence in the American market due to their integration into longstanding supply chains and their deployment across a range of critical sectors. Despite the FCC's previous actions, thousands of authorized devices, which contain components produced by Covered List entities, remain installed across the country, posing a critical national security threat.

To close these gaps, the FCC should adopt a more comprehensive set of regulations to efficiently remove equipment produced by entities on the Covered List from U.S. networks and infrastructure. This process should also occur over a transition period to moderate up-front costs while still encouraging American service providers to switch to components produced by U.S. allies and partners.

The FCC Should Close Longstanding Regulatory Loopholes

Chinese equipment continues to pose both an espionage and a sabotage threat to U.S. networks. Over the past half decade, Beijing has become more aggressive in targeting American critical infrastructure, including healthcare networks, utilities, and telecommunications, both to collect intelligence and to potentially introduce vulnerabilities that may be exploited in the event of a crisis with the United States.[1] These efforts have followed in parallel with China's cyber operations targeting the federal government, the American military, and defense contractors, which may have provided valuable intelligence or hindered Washington's capacity to deter or defeat Beijing if necessary.[2]

In response, the FCC has embraced its national security mission by recognizing that certain foreign adversaries pose systemic risks to the United States that cannot be fully addressed within the current structure of the Covered List, which historically has primarily targeted specific firms. Rather, the commission has focused on prohibiting the importation of entire classes of products whose manufacturers are predominantly located in China and other jurisdictions of concern

[1] Jack Burnham and Annie Fixler, "Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program," *Foundation for Defense of Democracies*, December 22, 2025. (https://www.fdd.org/analysis/2025/12/22/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the-equipment-authorization-program-2)
[2] Ibid.

while countering longstanding foreign ownership, control, or influence (FOCI) concerns via expansive screening criteria.[3]

These efforts have also extended to securing critical equipment supply chains, particularly in identifying and banning devices containing vulnerable components from entering the domestic market or connecting to critical networks. Through its most recent national security determinations on routers and drones, the commission has recognized that entire supply chains — from components to finished products — pose an unacceptable national security risk to the United States, rightly expanding the scope of further scrutiny and accompanying regulation.[4]

This focus has been anchored by congressional statute and federal jurisprudence, both within particular sectors, such as drones, and across the commission's regulatory jurisdiction covering networks and authorized products. Prior to the FCC's designation of all foreign-produced drones, the FY2025 National Defense Authorization Act established a process for excluding video and surveillance equipment related to drones produced by DJI and Autel Robotics from receiving equipment authorizations, highlighting a recognition of the dangers posed by subcomponents embedded within finished products entering the American market.[5] Under the Secure Networks Act (SNA) of 2019, Congress also ensured that the commission could bar finished products under a broad range of justifications, not limited to the capacity to interrupt communications systems, to protect U.S. national security.[6]

This power was reaffirmed in *Huawei Technologies USA, Inc. v. FCC*, a decision that strengthened the commission's hand in applying national security criteria to its regulatory decisions, even absent explicit congressional authority for specific regulatory actions under SNA.[7] Although more limited, this reach can also practically extend to dangerous software products embedded within imported devices — the FCC prohibited authorization of equipment including Kaspersky antivirus software from the American market due to national security concerns related to its ties to Moscow and its backdoor vulnerabilities.[8]

---

[3] Federal Communications Commission, Public Notice, "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," December 22, 2025. (https://docs.fcc.gov/public/attachments/DA-25-1086A1.pdf)

[4] Ibid.; Federal Communications Commission, Public Notice, "FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List," March 23, 2026. (https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf)

[5] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. 118-159, §1709, 138 Stat. 1773, 2209-2210. (https://www.congress.gov/bill/118th-congress/senate-bill/4638/text)

[6] Secure and Trusted Communications Networks Act of 2019, Pub. L. 116-124, 134 Stat. 158, codified as amended at 47 U.S.C. §§1601-1609. (https://www.congress.gov/116/plaws/publ124/PLAW-116publ124.pdf)

[7] *Huawei Technologies USA, Inc. v. FCC, 2 F.4th 421* (5th Cir. 2021). (https://www.ca5.uscourts.gov/Opinions/pub/19/19-60896-CV0.pdf)

[8] Federal Communications Commission, Public Notice, "Office of Engineering and Technology and Public Safety and Homeland Security Bureau Announce Prohibition on Authorization of Equipment That Includes Kaspersky Cybersecurity or Anti-Virus Software," September 3, 2024. (https://docs.fcc.gov/public/attachments/DA-24-886A1.pdf)

However, the FCC's current use of certain regulatory tools, even those built on strong statutory authorities, may inadvertently complicate compliance while opening dangerous gaps. Combining firm-specific and region-specific restrictions into a single list may complicate efforts to account for complex supply chains — certain routers or drones may be authorized by one set of standards but contain too many foreign-sourced components to qualify as a domestically produced product, restricting their importation. Moreover, the differing standards among the Department of Homeland Security, the Pentagon, and the commission for approving conditional licenses for foreign-produced products that would otherwise be barred may inadvertently slow efforts to securely source key supply chains.

The commission also suffers from key reporting gaps that complicate its enforcement actions. While products are required to undergo testing at FCC-recognized facilities to receive an equipment authorization, manufacturers are not required to disclose the origin or producer of all non-radio-frequency components — a gap the commission only partially closed within its Third Order and Report by focusing on logic-bearing hardware produced by Covered List entities.[9] Notably, this gap is even more significant in the software sector, as the Kaspersky incident remains the FCC's only successful effort to list a software product as a national security threat.[10] As such, the commission cannot fully ascertain the risk profile posed by each authorized piece of equipment, posing a key national security risk.

Recommendations

The FCC should pursue a series of measures to tighten its standards during the equipment authorization process. These should include preventing any component produced by a Covered List entity or sector from entering the domestic market by enhancing scrutiny over the entire production process, including requiring applicants to submit both a hardware and a software bill of materials (HBOM and SBOM) to provide greater clarity regarding a device's technical structure. The commission should also work to prevent firms from circumventing these restrictions by closing white-listing loopholes, requiring notifications for software and firmware updates, and streamlining the revocation process for equipment authorizations.

[9] Federal Communications Commission, "Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, Third Report and Order and Third Further Notice of Proposed Rulemaking," July 23, 2026. (https://docs.fcc.gov/public/attachments/FCC-26-50A1.pdf)
[10] Federal Communications Commission, Public Notice, "Office of Engineering and Technology and Public Safety and Homeland Security Bureau Announce Prohibition on Authorization of Equipment That Includes Kaspersky Cybersecurity or Anti-Virus Software," September 3, 2024. (https://docs.fcc.gov/public/attachments/DA-24-886A1.pdf)

- **The FCC should codify its definition of "produced by" to prevent Covered List devices from entering the United States.** The commission should define "produced by" to include any entity that exercises substantial responsibility for, or control over, any major stage of the process by which the device comes into existence, including the design, manufacturing, assembly, or development of the device. Notably, this definition should provide protection against Covered List entities operating deep within the supply chain while allowing U.S. firms to source design intellectual property from abroad so long as they maintain control of key security elements. This should include exclusive design control and exclusive authority over compilation, cryptographic signing, and delivery of firmware and updates for the device's logic-bearing subsystems; prohibiting third-party update pathways; and providing independent security evaluations.

- **The FCC should pursue a staggered approach to prohibiting authorization for devices incorporating any components produced by a Covered List entity or Covered List sector**. Under direct authority from the SNA and supported by both Executive Order 13873 and the commission's national security determinations, the FCC should prohibit any device containing components from a Covered List entity or sector from receiving an equipment authorization. This prohibition should extend to hardware, firmware, and software — beyond the logic-bearing components or RF-connected threshold adopted previously. However, given both the up-front and recurring costs of this proposal, the FCC should consider implementing a staggered approach, either by lengthening compliance timelines or by targeting components embedded within critical infrastructure as defined by 42 U.S.C. § 5195c(e).

- **The FCC should require equipment authorization applicants to submit an HBOM and an SBOM at the time they apply for certification and require grantees to update the commission on any changes to the HBOM or SBOM of the device.** Under the statutory authority provided by the Secure Networks Act and the Secure Equipment Act, the commission should require applicants to disclose all components of a device, including the producer of each component, the location of each component's production, and the percentage of component value associated with each production location. This rule is critical for enforcing Covered List prohibitions, particularly Covered List sector restrictions, and offers insight into potential vulnerabilities.

- **The FCC should close potential loopholes in the white-labeling process by requiring equipment authorization applicants to disclose all known "electrically identical" products.** Current commission regulations allow a firm to white-label an existing authorized device that is "electrically identical" under its own FCC ID without resubmitting to equipment testing — a vulnerability that allows entities to introduce discrete but potentially significant vulnerabilities into these products. Moreover, this

process also ensures that if a product's equipment authorization is later revoked, the FCC cannot readily identify its licensed versions due to differentiation among model and FCC ID. As such, the commission should require that all applicants disclose all "electrically identical" products to allow for cross-referencing these products in the event of a revocation of their authorizations.

- **The FCC should clarify and tighten its definition of "produced in a foreign country" to secure critical technology supply chains.** To ease the regulatory burden on importers and producers, the commission should adopt a simplified definition to determine whether a device is "produced in a foreign country." To qualify, a device must not meet the criteria of a "domestic end product" as defined in 48 CFR 25.101(a)(1). However, the FCC should also develop a subset of this definition to specifically target products whose manufacturing, assembly, design, and development occurred within a "covered nation" under 10 U.S.C. § 4872(d)(2). These products should be subject to a higher level of regulatory scrutiny, including a presumption of denial for conditional authorization.

- **The FCC should amend sections 2.932(b) and 2.1043(b) of its equipment authorization rules to mandate that minor software and firmware security updates to all currently valid equipment authorizations held by Covered List entities and Covered List sectors require a new authorization proposal**. The commission noted in PS Docket No. 26-72 that previously authorized equipment produced by Covered List entities and sectors poses an unacceptable national security risk, as it is "often functionally identical to these firms' more recently banned products." To counter these risks, the commission should consider screening security patches while allowing for routine maintenance updates.

- **The FCC should adopt a streamlined revocation procedure.** The commission should copy its equipment authorization revocation process as articulated in its First Report and Order on submarine cables to prioritize national security determinations within its procedures. Grounds for revocation should include willful false statements or misrepresentations to the commission, test labs, DHS, or the Pentagon as part of an application for, or maintenance of, a conditional approval.

- **The FCC should consider imposing a uniform automatic expiration date for all equipment authorizations.** While the commission has previously sought to revoke prior equipment authorizations due to national security concerns, this process remains rooted in countering specific vulnerabilities rather than addressing the system as a whole. A uniform expiration date would formalize this process by allowing the commission to reconsider the national security implications of emerging risks.

- **The FCC should require that every applicant or grantee for FCC-certified equipment have a U.S.-based liable party.** While the commission can impose penalties for violating its regulations, many offenders are effectively located beyond its jurisdiction, limiting the penalties' efficacy in deterring such behavior. As such, the FCC should identify a U.S.-based liable party in granting equipment authorizations — the U.S.-based manufacturer, importer, retailer, or entity involved in unlicensed modifications.

- **The FCC should strengthen its accredited test lab ecosystem.** The FCC's efforts to increase scrutiny over high-risk components, adopt an HBOM/SBOM requirement, and address white-listing fraud will depend on a rigorous, well-resourced testing environment. To that end, the commission should consider new funding avenues for test labs and stronger coordination mechanisms with labs in allied and partner nations to expand capacity without sacrificing the agency's previous efforts to remove "bad labs."

Conclusion

By increasing transparency and strengthening layered supply-chain accountability, the commission can bolster Washington's national security posture while supporting continued innovation in the telecommunications industry. The cost of inaction, particularly as the FCC seeks to limit other avenues for foreign adversaries to access U.S. networks, signals that existing regulatory loopholes can be exploited to maintain access to critical infrastructure.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into the commission's ongoing policy work.