Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New FCC Router Rule Signals Shifting Supply Chain Approach

By **Loyaan Egal, JiaZhen Guo and Leetal Weiss** (April 23, 2026, 4:38 PM EDT)


Loyaan Egal


Jiazhen Guo


Leetal Weiss

The Federal Communications Commission's recent addition of consumer-grade routers newly produced outside of the U.S. to its covered list marks another notable expansion of the Trump administration's supply chain risk regulation and national security policy.

This addition became effective March 23, and prohibits the authorization and use of newly produced covered routers unless a conditional approval is granted by the U.S. Department of Defense or the U.S. Department of Homeland Security.

Because this new category is defined by place of production rather than by manufacturer identity, its implications extend beyond any particular company and may signal broader future action affecting other classes of equipment.

The development also creates immediate reporting, certification and procurement considerations for advanced communications service providers, which should promptly review sourcing practices, contractual arrangements and related FCC certification obligations. Additionally, it represents the second time in three months that the FCC has categorically expanded the covered list, with the first such action involving all foreign-made uncrewed aircraft systems, or UAS, and their critical components.

This marks what appears to be a policy shift in which the Trump administration has begun to use the FCC's covered list in place of the U.S. Department of Commerce's Information and Communications Technology and Services, or ICTS, supply chain risk regulations, as well as authorities under Trump's 2019 Executive Order No. 13873 on securing information and communications technology and services against foreign adversaries, to address certain supply chain and national security risks.

Background

On March 23, the FCC's Public Safety and Homeland Security Bureau issued a public notice adding consumer-grade routers produced in a foreign country to the FCC's covered list. This includes consumer-grade networking devices that are primarily intended for residential or small office/home office use and can be installed by the customer, rather than enterprise-grade routing infrastructure.[1]

Similar to the FCC's categorical action targeting foreign-made drones and drone critical components,[2]

as well as the FCC's proposal to include certain connected vehicle hardware and software,[3] this action targets foreign-made routers based solely on their place of production instead of specific entities or manufacturers.

FCC Covered List Addition: Scope and Process

Under the Secure and Trusted Communications Networks Act, the FCC cannot, of its own volition, add entities and their services and equipment to the covered list.

It has to rely on a specific determination made by a limited category of bodies: (1) any executive branch interagency body with appropriate national security expertise; (2) the Commerce Department pursuant to Executive Order No. 13873; (3) covered communications equipment or services identified in the National Defense Authorization Act; or (4) an appropriate national security agency, including DHS and the DOD.[4]

The last two additions to the covered list, including drones and consumer-grade routers, were based on a specific determination made by a White House-convened executive branch interagency body with national security expertise.

This is a departure from past determinations that were made by the likes of Team Telecom (formally the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector), the Commerce Department under Executive Order No. 13873's ICTS supply chain risk authorities, or through entities identified in the National Defense Authorization Act.

This is the second such action the current FCC has taken (i.e., using a White House-convened interagency body with national security expertise to make a categorical determination), with the first occurring in December 2025 and involving all foreign-made UAS and UAS components.

Under FCC equipment authorization rules, devices placed on the covered list are ineligible to receive a grant of certification from a Telecommunication Certification Body; cannot be marketed or imported in the U.S.; and cannot be purchased, maintained or operated using FCC-administered subsidies, while companies must annually certify to the FCC that their products are not prohibited covered equipment.

The ban on newly produced foreign consumer-grade routers is currently in effect and applies to all newly produced consumer-grade routers made outside of the U.S. after March. It does not, however, apply to existing routers (i.e., any items produced before March 2026).

However, the FCC has initiated a proceeding proposing to prohibit the continued importation and marketing of certain previously authorized covered communications equipment added to the covered list in 2024 or earlier,[5] which suggests that the agency may take a similar approach here as well.

Conditional Approval Pathway

The FCC provides a pathway for continued participation of new foreign-produced routers in the U.S. market through what it terms a "conditional approval" process. Entities that produce covered routers outside the U.S. may apply to the DOD or DHS for a conditional approval.

If granted, the relevant router or class of routers would be exempt from the covered list restriction and could continue to seek an FCC authorization during the approval period. Conditional approvals may be

granted for periods of up to 18 months.

To obtain a conditional approval, applicants must provide the following:

- Corporate structure information, including about ownership, parents, subsidiaries, affiliates, beneficial owners of 5% or more, the board, and executive information, as well as any foreign government ownership, control, influence, financing or material support;

- Manufacturing and supply chain information, including a detailed bill of materials, country of origin for components and design, responsibility for intellectual property ownership and software updates, manufacturing, assembly and testing locations, software and firmware origin, supply chain concentration by country, and any single points of failure; and

- A U.S. manufacturing and onshoring plan, including a time-bound road map to establish or expand U.S. manufacturing, the responsible point of contact, current U.S. footprint, planned capital expenditures and investments, and, where applicable, progress made under prior conditional approval commitments.

Submission does not guarantee approval, and only routers receiving conditional approvals are exempt from the covered list restriction for the approval period.

Advanced Communications Service Providers Reporting and Certification Obligations

Providers of advanced communications services[6] are required to report and certify annually whether they have purchased, rented, leased or otherwise obtained any covered communications equipment or services on the FCC's covered list via the FCC supply chain annual reporting requirement.[7] This report is due March 31 of each year and must cover information as of Dec. 31 of the preceding year.

If in instances such as these where the FCC adds equipment or services to the covered list, filers are required to report any equipment or services obtained 60 days or more after the date they were added to the covered list.

Although the FCC has not provided specific guidance on this issue, it appears that the reporting obligation would now extend to advanced communications service providers utilizing new foreign consumer-grade routers covered by the new rule.

Apparent Shift From ICTS Supply Chain Risk Authorities to the Covered List

Both UAS/drones[8] and small office/home office routers[9] were items that the Commerce Department's Office of Information and Communications Technology and Services was preparing to regulate under its Executive Order No. 13873 ICTS supply chain risk authorities. Both of those categories of concern were recently addressed through the FCC covered list process.

It remains to be seen if there are other categorical sectors that the Trump administration will choose to regulate through the covered list process. For instance, the Office of Information and Communications Technology and Services was also working on regulations related to networking equipment and services in data centers.[10]

The recent substitution of Commerce's Executive Order No. 13873 supply chain risk tools with the

covered list as a means to address perceived national security risks and advance U.S. domestic manufacturing and supply chain policy priorities leaves open the possibility of further actions that might take a categorical and industry-specific, entity-agnostic approach.

Next Steps

The FCC's action requires immediate attention from manufacturers, carriers and service providers:

- Companies purchasing, maintaining or operating consumer-grade routers produced outside the U.S. should evaluate router procurement and deployment strategies, review pending or future FCC filings and certifications, and consider preparing conditional approval submissions.

- Particular focus should be placed on the national security determinations indication of "production," which includes manufacturing, assembly, design and development.

- Entities seeking conditional approval should begin preparing comprehensive documentation covering corporate structure, manufacturing and supply chain operations, and U.S. manufacturing and onshoring plans.

- Providers of advanced communication services should review reporting requirements to ensure timely and accurate reporting and certifications under FCC rules, reflecting the addition of consumer-grade routers to the covered list.

The Trump administration's recent use of the covered list as a preferred tool to address ICTS supply chain and national security risks, coupled with the FCC's addition of foreign-produced consumer-grade routers to its covered list, represents a substantial shift in supply chain security policy, directly affecting manufacturers, carriers and service providers.

Immediate review of procurement, authorization and compliance practices is essential to navigate the new restrictions and reporting obligations. Companies should monitor developments regarding conditional approval processes and broader supply chain policy initiatives, as further categorical additions to the covered list remain a distinct and real possibility.

Loyaan A. Egal is a partner at Morgan Lewis & Bockius LLP. He previously served at the FCC as special adviser to former FCC Chair Jessica Rosenworcel, chief of the agency's Enforcement Bureau, and head of its privacy and data protection task force.

JiaZhen Guo is an associate at the firm.

Leetal Weiss is an associate at the firm.

[1] U.S. Dep't of Commerce, Nat'l Institute of Standards and Tech., Recommended Cybersecurity Requirements for Consumer-Grade Router Products, NIST IR 8425A, at 1 (Sept. 2024).

[2] Public Notice, Fed. Commc'ns Comm'n, Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Aboard, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List (Dec. 22, 2025).

[3] Public Notice, Fed. Commc'ns Comm'n, The Public Safety and Homeland Security Bureau and the Office of Engineering and Technology Seek Public Input on Commerce Department Determination Regarding Certain Connected Vehicle Technologies (May 23, 2025).

[4] 47 U.S.C. §§ 1601(c), 1608(2).

[5] Public Notice, Fed. Commc'ns Comm'n, Public Safety and Homeland Security Bureau and the 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 (Mar. 27, 2026).

[6] 47 CFR § 1.50001.

[7] 47 U.S.C. § 1604; 47 CFR § 1.50007.

[8] Advance Notice of Proposed Rulemaking, Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems, US Dep't of Commerce, 90 Fed. Reg. 271 (Jan. 3, 2025).

[9] Agency Rule List – Spring 2025, Interim Final Rule, Securing the Information and Communications Technology and Services Supply Chain: Communications and Networking Devices, US Dep't of Commerce (Spring 2025).

[10] Agency Rule List – Spring 2025, Interim Final Rule, Securing the Information and Communications Technology and Services Supply Chain: Networking Equipment and Services in Data Centers, US Dep't of Commerce (Spring 2025).