Cooley

FCC Moves to Prevent New Foreign Routers

March 26, 2026

On March 23, 2026, the FCC's Public Safety and Homeland Security Bureau took the sweeping step of adding all "routers produced in a foreign country" to the FCC's Covered List. This action follows a national security determination that these devices –specifically those intended for residential or "small office/home office" use – pose an unacceptable risk to US infrastructure. This action takes effect immediately.

The determination explicitly links foreign-produced routers to recent high-profile cyber campaigns, including Volt Typhoon and Salt Typhoon, which targeted American energy and water systems. By placing these products on the Covered List, the FCC is effectively preventing any new foreign-produced router models from being authorized for sale or marketing in the US.

Products that are on the Covered List cannot receive FCC authorizations; therefore, any routers that were previously approved can continue to be sold in the US, but no new foreign-produced routers can be marketed or sold in the US without a waiver. Companies that produce routers outside the US can seek conditional waivers from the Department of War or Department of Homeland Security (DHS). The FCC also announced an additional waiver that permits previously authorized routers to receive basic software and firmware updates to maintain usability until March 1, 2027. Finally, the FCC released an FAQ with more information about the effect of its action to add foreign-produced routers to the Covered List.

The FCC defined "routers" to mean consumer-grade networking devices that are primarily intended for residential use and can be installed by the customer. Routers forward data packets, most commonly Internet Protocol packets, between networked systems. The FCC also defined "production" broadly to include any significant stage of the process by which the device is made, including manufacturing, assembly, design and development.

This latest action follows several other recent FCC efforts to mitigate perceived undue risks raised by foreign actors. For example, the FCC recently banned drones manufactured outside the US, withdrew recognition from several test labs and implemented stringent disclosure requirements for entities with ties to foreign adversaries.

Practical actions for affected companies

If your company manufactures, distributes or integrates these products, you should consider the following immediate steps:

1. **Audit your roadmap and supply chain**

- **Identify country of origin**: Determine exactly where your current router inventory and future pipeline are manufactured. Under the new rule, even "American" brands may be affected if their physical production occurs in a foreign country.
- **Assess "foreign-produced" models**: If only minor assembly of a product happens abroad, you may be able to demonstrate that it should not be on the Covered List.
- **Identify "previously authorized" models**: Confirm which of your foreign-produced models already have an approved FCC ID. These can still be imported and sold.
- **Pipeline review:** Any new models (e.g., upcoming Wi-Fi 7 releases) currently in development abroad will likely be blocked from the U.S. market unless you pivot your manufacturing strategy.

2. **Apply for 'conditional approval'**

The FCC has provided a pathway for exemptions through the Department of War and DHS. To succeed, applicants should be prepared to provide:

- A detailed bill of materials and country of origin for all components.
- A US manufacturing and onshoring plan that is time-bound and overseen by a dedicated officer.
- Quarterly updates on the progress of bringing production to US soil.

3. Secure your legacy fleet

Take advantage of the FCC Office of Engineering and Technology waiver. This allows previously authorized routers to receive software and firmware updates to mitigate security harms. This waiver is currently set to expire on March 1, 2027. Ensure you have a plan to push security updates to existing foreign-made routers before the waiver window potentially narrows or expires.

4. Update certifications

Going forward, all applicants for FCC equipment authorization who have a product on the “covered list” will need to self-certify, in good faith, that their device is not “covered equipment.” False certifications could lead to significant legal exposure and the revocation of existing authorizations.

How we can help

The landscape for telecommunications equipment is shifting toward a “buy American” or “produce American” mandate. If you have questions about the conditional approval application process, need assistance analyzing how this action impacts your current inventory or would like to explore legal challenges, please reach out to the Cooley lawyers listed below.

Key Contacts

Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018
Henry Wendel Washington, DC	hwendel@cooley.com +1 202 776 2943
J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818

Ronald W. Del Sesto Washington, DC	rdelsesto@cooley.com +1 202 728 7128
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Brett P. Ferenchak Washington, DC	bferenchak@cooley.com +1 202 776 2138
Zhijing Yu Singapore	zyu@cooley.com +65 6962 7527