wiley

ALERT

FCC Adds Foreign-Produced Consumer-Grade Routers to Covered List

March 24, 2026

***UPDATE*: On April 1, 2026 we published an update to this alert here.**

On March 23, 2026, the Federal Communications Commission (FCC) added all foreign-produced consumer-grade routers to its Covered List of communications equipment and services deemed to pose an unacceptable risk to U.S. national security. The addition to the Covered List means that covered routers cannot receive any new FCC radiofrequency equipment authorizations. Although pre-existing authorizations for covered routers will continue to be valid unless the FCC takes further action to revoke or limit them, changes to previously authorized routers are generally prohibited. Critical firmware and software updates are permitted pursuant to a blanket waiver issued by the Office of Engineering and Technology (OET).

The router addition to the Covered List is similar to the entry for uncrewed aircraft systems (UAS) and UAS critical components issued in December 2025. Notably, like the drone entry, the router entry covers all consumer-grade routers "produced in a foreign country," not just those produced in foreign adversary countries or by entities linked to foreign adversaries. In addition, the FCC adopted a comparable Conditional Approval process, whereby affected entities can apply for approval from the Department of Homeland Security (DHS) or the Department of War (DoW) to be exempt from the Covered List for a period of time. The underlying national security determination that spurred the Covered List update encourages affected parties to seek Conditional Approval. Language in OET's waiver further suggests that some type of categorical exemption from DoW, similar to the "Blue UAS" and "Buy American" exemptions in the drone Covered List entry, may be forthcoming.

Authors

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Sara M. Baxenberg
Partner
202.719.3755
sbaxenberg@wiley.law

Matt Lapin
Of Counsel
202.719.3435
mlapin@wiley.law

Joshua S. Turner
Partner
202.719.4807
jturner@wiley.law

Practice Areas

Emerging Technologies
National Security
Telecom, Media & Technology
Trump Administration Resource Center
Uncrewed Aircraft Systems (UAS)

The Covered List Router Entry. The addition to the Covered List follows a National Security Determination (Determination) dated March 20, 2026 concluding that routers produced in foreign countries pose an unacceptable risk to national security. The FCC's Public Notice indicates that "the White House convened an Executive Branch interagency body with national security expertise" pursuant to the Secure Networks Act, but does not identify which federal agencies participated. The Determination explains that "[c]ompromised routers can enable in-depth network surveillance data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses' networks," and further notes that foreign-produced routers "were directly implicated in the Volt, Flax, and Salt Typhoon cyberattacks which targeted critical American communications, energy, transportation, and water infrastructure." The Determination identifies the following national security risks posed by foreign-produced routers: "(1) introducing a supply chain vulnerability that could disrupt the U.S. economy, critical infrastructure, and national defense; and (2) establishing a severe cybersecurity risk that could be leveraged to immediately and severely disrupt U.S. critical infrastructure and directly harm U.S. persons."

The Determination discusses potential threats to "homes, businesses, critical infrastructure, and emergency services" from foreign-produced routers. But despite this broad threat analysis, the Determination makes clear that this action is limited to consumer-grade routers:

> For the purpose of this determination, the term "Routers" is defined by National Institute of Science and Technology's Internal Report 8425A to include 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 (IP) packets, between networked systems.

The Determination further sheds light on how to determine the location of production, explaining that "[p]roduction generally includes any major stage of the process through which the device is made, including manufacturing, assembly, design, and development."

The FCC concluded that it was required to add foreign-produced routers to the Covered List pursuant to the Secure Networks Act, which directs the agency to compile the Covered List using "specific determinations" made by federal agencies and interagency bodies with relevant national security expertise. In addition to updating the Covered List to include routers, the FCC published an FAQ on its action here.

OET Blanket Waiver Allowing Class I Permissive Changes. When equipment is added to the Covered List, previously granted equipment authorizations continue to be valid unless and until the FCC takes some affirmative step related to those authorizations. However, changes to the equipment – including what the FCC calls "Class I permissive changes," which ordinarily can be made without seeking any approval – are prohibited. That can include changes and updates to software as well as hardware, potentially cutting off updates to devices that have already been certified.

To address this problem, OET issued a blanket waiver on March 23 to enable Class I permissive changes to previously authorized covered routers, specifically for "software and firmware updates that mitigate harm to U.S. consumers." These include "software and firmware updates to ensure the continued functionality of the

devices, such as those that patch vulnerabilities and facilitate compatibility with different operating systems." The waiver will be in place "at least until March 1, 2027." OET granted the same kind of waiver to covered UAS and critical components in January 2026.

Availability of Conditional Approvals. Also like the drone entry, the FCC plans to allow entities to seek "Conditional Approval" from DoW and DHS to exempt otherwise-covered routers and allow them to receive new equipment authorizations. Notably, the Determination itself emphasized the availability of Conditional Approvals and "encouraged" entities that produce covered routers to apply for them. The FCC appended as an Annex to its Public Notice a guidance document on submission criteria for Conditional Approvals. Like the analogous guidance for Conditional Approvals of covered drones and components, the guidance provided for routers explains that entities seeking Conditional Approval must submit information regarding their corporate structure, foreign ownership, supply chains, and onshoring plans for manufacturing the covered product. (The FCC announced the first round of Conditional Approvals for covered drones and components last week.)

Potential Exemption from DoW. The router Covered List entry extends to all "routers produced in a foreign country, except routers which have been granted a Conditional Approval by DoW or DHS" (no such approvals have been issued yet). The OET waiver, however, indicates that some type of categorical exemption could be forthcoming. In electing March 1, 2027 as the expiration for the blanket waiver, OET's Public Notice explains that "March 1, 2027, is convenient because it is the date until which the recent DoW determination excepts certain otherwise Covered Routers." There is no "DoW determination" included in the FCC's Covered List update, and the determination that *was* included (by the "interagency body") does not reference an exception until March 1, 2027 for certain routers. Further, OET does not appear to be referencing future Conditional Approvals issued by DoW, as the FCC's guidance for seeking Conditional Approval of covered routers indicates that such approvals can be granted for a period of up to 18 months, which is well past March 1, 2027.

OET's discussion of the March 1 deadline suggests that a DoW determination exempting certain routers or classes of routers over that period may be forthcoming. In the context of the UAS update (which also began with an "interagency body" determination), DoW issued a determination shortly after the entry was added to exempt, until January 1, 2027, all UAS and critical components that are included on the Defense Contract Management Agency's (DCMA) "Blue UAS" lists or that satisfy the "Buy American" country of origin standard used in trade law. Interested stakeholders should monitor closely for a comparable, time-bound exemption here.

FCC Action Is Consistent with Broader U.S. Supply Chain Security Approach. The FCC determination is consistent with prior assessments by other U.S. government agencies regarding national security risks posed by foreign produced routers. Media reports have indicated that the Department of Justice, in coordination with the DoW and the Department of Commerce's Bureau of Industry and Security (BIS), previously initiated investigations into the use of routers in the cyberattacks noted above. The House Select Committee on the Chinese Communist Party had also previously requested that BIS, through its Office of Information and Communications Technology and Services (OICTS), investigate risks posed by such routers. BIS had also previously issued a notice of its intent to issue an interim rule through OICTS that would address national

security risks of foreign produced items integral to communications and networking devices, including routers. Although this rule has not been published to date, if BIS believes the FCC determination does not fully address the risks identified, it is possible that such rule or other regulatory actions may still be undertaken.