Steptoe

FCC Adds Foreign-Produced Routers to the Covered List

On March 23, 2026, the FCC's Public Safety and Homeland Security Bureau added routers produced in a foreign country to the Covered List (Public Notice, DA 26-278). Routers forward data packets, most commonly Internet Protocol (IP) packets, between networked systems.

This action followed a National Security Determination ("NSD") by the Executive Branch that foreign-made routers pose unacceptable national security risks. Among other reasons, the NSD cited threats to critical networking infrastructure and cyberattacks by foreign manufactured routers.

The FCC's Covered List identifies communications equipment and services deemed to pose an unacceptable risk to U.S. national security. *See* 47 U.S.C. 1601(a). Equipment included on the list cannot receive a new FCC equipment authorization, which can prevent new models from being imported, marketed, or sold in the United States. *See* 47 C.F.R. § 2.903(a). Applicants seeking equipment authorization from the FCC must certify that a device is not on the Covered List. 47 C.F.R. § 2.911(d)(5)(i).

What is a covered router?

The NSD required the FCC to place routers produced in a foreign country, regardless of the nationality of the producer, on the Covered List "unless the Department of War (DoW) or the Department of Homeland Security (DHS) transmits to the FCC a specific determination that a given router or class of routers do not pose" a national security risk.

The NSD defines routers as "consumer-grade networking devices that are primarily intended for residential use and can be installed by the customer."

ISP-provided residential gateways that combine modem and router functions in a single device fall within the scope of the determination.

The NSD clarifies that "production generally includes any major stage of the process through which the device is made, including manufacturing, assembly, design, and development."

Effect on existing equipment

Routers will be prohibited from receiving FCC authorization to be imported, marketed, or sold in the United States, unless a conditional authorization is obtained. However, existing routers that the FCC previously authorized can continue to be imported and sold. Devices that consumers previously purchased are likewise unaffected.

The FCC's Office of Engineering and Technology (OET) issued a waiver for existing authorized routers to be able to receive software and firmware updates through at least January 1, 2029. 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.

Obtaining Conditional Approval for Covered Routers

Entities wishing to import covered routers can request an exemption from the Covered List by receiving a "conditional approval." DoW or DHS will make a specific determination to the FCC that a given router or class of routers (e.g., routers produced by a specified entity) do not pose unacceptable risks to national security.

The FCC itself has no discretion in this process, as the determination on whether to grant the conditional approval is made solely by either DoW or DHS. Conditional approvals will be granted for up to 18 months.

The conditional approval application must include the following categories of information:

Corporate Structure:

- legal name, jurisdiction of incorporation, and principal place of business;
- ownership structure, including parents, subsidiaries, affiliates, and joint ventures;
- beneficial owners holding at least five percent equity;
- board members and executive leadership, including nationality and country of residence; and
- foreign government ownership, control, influence, financing, or material support (including any arrangements that allow foreign persons or governments to influence operations, decision-making, or access to technology.)

Manufacturing and Supply Chain:

- a detailed bill of materials;
- country of origin for all components, software, and firmware in the router;
- entities responsible for IP ownership and software updates for the router;
- justification for why the device is not currently manufactured in the United States, including why the foreign country was selected and whether alternatives exist;
- manufacturing, final assembly, and testing locations;
- quantitative assessment of supply chain concentration by country, as both a percentage of total value and production volume; and
- identification of any single points of failure in the supply chain including sole source suppliers, the country of those sole-source suppliers, and a description of contingency plans if those suppliers become unavailable.

U.S. Manufacturing and Onshoring Plan

- a detailed, time-bound plan to establish or expand manufacturing in the United States;

- a point of contact responsible for implementing and overseeing the U.S. manufacturing and onshoring plan;
- a description of existing U.S.-based manufacturing and assembly including: percentage of components assembled in the United States and current U.S. headcount and facilities;
- a description of committed and planned capital expenditures, financing, or other investments dedicated to U.S.-based manufacturing and assembly over the next 1-5 years, including expected timelines and milestones (including additional number of employees expected to be hired and expected expansion of domestic manufacturing facilities); and
- an inventory of the progress made on the U.S. manufacturing and onshoring plans submitted for all prior covered list approvals.

The FCC has periodically updated the covered list to account for conditional approvals.

Next Steps

Steptoe's Telecom and International Trade attorneys can help steer companies that have covered routers through the conditional approval process. For more information, please contact one of the authors.