NEWS FROM THE FEDERAL COMMUNICATIONS COMMISSION

FACT SHEET: FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models

Update Follows Determination by Executive Branch Agencies that Consumer-Grade Routers Produced in Foreign Countries Threaten National Security

WASHINGTON, March 23, 2026—Today, the Federal Communications Commission updated its Covered List to include all consumer-grade routers produced in foreign countries. Routers are the boxes in every home that connect computers, phones, and smart devices to the internet. This followed a determination by a White House-convened Executive Branch interagency body with appropriate national security expertise that such routers "pose unacceptable risks to the national security of the United States or the safety and security of United States persons."

The Executive Branch determination noted that foreign-produced routers (1) introduce "a supply chain vulnerability that could disrupt the U.S. economy, critical infrastructure, and national defense" and (2) pose "a severe cybersecurity risk that could be leveraged to immediately and severely disrupt U.S. critical infrastructure and directly harm U.S. persons."

President Trump's 2025 National Security Strategy stated: "the United States must never be dependent on any outside power for core components—from raw materials to parts to finished products—necessary to the nation's defense or economy. We must re-secure our own independent and reliable access to the goods we need to defend ourselves and preserve our way of life."

Malicious actors have exploited security gaps in foreign-made routers to attack American households, disrupt networks, enable espionage, and facilitate intellectual property theft. Foreign-made routers were also involved in the Volt, Flax, and Salt Typhoon cyberattacks targeting vital U.S. infrastructure.

The determination included an exemption for routers that the Department of War (DoW) or the Department of Homeland Security (DHS) have granted "Conditional Approval" after finding that such device or devices do not pose such unacceptable risks. Producers of consumer-grade routers are encouraged to submit an application for Conditional Approval using the guidance attached to the determination. Applications should be submitted to conditional-approvals@fcc.gov.

As outlined below, today's action does not impact a consumer's continued use of routers they previously acquired. Nor does it prevent retailers from continuing to sell, import, or market router models approved previously through the FCC's equipment authorization process. By operation of the FCC's Covered List rules, the restrictions imposed today apply to new device models.

Chairman Carr issued the following statement:

"I welcome this Executive Branch national security determination, and I am pleased that the FCC has now added foreign-produced routers, which were found to pose an unacceptable national security risk, to the FCC's Covered List. Following President Trump's leadership, the FCC will

continue to do our part in making sure that U.S. cyberspace, critical infrastructure, and supply chains are safe and secure."

Additional Background:

- The FCC's Covered List is a list of communications equipment and services that are deemed to pose an unacceptable risk to the national security of the U.S. or the safety and security of U.S. persons.
- Under the Secure and Trusted Communications Networks Act, the Commission can update the Covered List only at the direction of national security authorities. In other words, the Commission cannot update this list on its own and is required to implement determinations that are made by our national security agency experts.
- Equipment on the Covered List ("covered" equipment) is prohibited from getting FCC equipment authorization. Most electronic devices (including consumer-grade routers) require FCC equipment authorization prior to importation, marketing, or sale in the U.S. Covered equipment is banned from receiving new equipment authorizations, preventing new devices from entering the U.S. market.
- The Cybersecurity and Infrastructure Security Agency encourages organizations to use the Covered List for risk management analysis in their regulatory compliance efforts.
- Following a similar National Security Determination in December, and a follow-up Determination in January, the FCC recently added the following to the Covered List: "Uncrewed aircraft systems (UAS) and UAS critical components produced in a foreign country†† —except, (a) UAS and UAS critical components included on the Defense Contract Management Agency's (DCMA's) Blue UAS Cleared List, until January 1, 2027,# (b) UAS critical components that qualify as "domestic end products" under the Buy American Standard, 48 CFR 25.101(a), until January 1, 2027; and (c) devices which have been granted a Conditional Approval by DoW or DHS—and all communications and video surveillance equipment and services listed in Section 1709(a)(1) of the FY25 National Defense Authorization Act (Pub. L. 118-159)".

What does this mean?

- **New** devices on the Covered List, such as foreign-made consumer-grade routers, are prohibited from receiving FCC authorization and are therefore prohibited from being imported for use or sale in the U.S. This update to the Covered List does not prohibit the import, sale, or use of any existing device models the FCC previously authorized.
- **This action does not affect any previously-purchased consumer-grade routers.** Consumers can continue to use any router they have already lawfully purchased or acquired.
- Producers of consumer-grade routers that receive **Conditional Approval** from DoW or DHS can continue to receive FCC equipment authorizations. Interested applicants are encouraged to submit applications to conditional-approvals@fcc.gov.

For more information, please see our FAQ page.

###

Media Contact: MediaRelations@fcc.gov / (202) 418-0500
@FCC / www.fcc.gov