FCC Router Ruling: Briefing Note

LOXADA™
SAFE, SECURE, REMOTE

What the March 23, 2026 FCC Covered List update means. And what it doesn't

WHAT HAPPENED

On March 23, 2026, the FCC updated its Covered List to include all consumer-grade routers produced in foreign countries. This followed a formal national security determination by a White House-convened interagency body, which the FCC is legally required to implement. The determination found that foreign-produced routers pose unacceptable risks to US national security and critical infrastructure.

The action was explicitly linked to documented attacks on US infrastructure, including the Volt, Flax, and Salt Typhoon intrusion campaigns, all of which exploited foreign-made network edge devices.

WHAT HAS CHANGED

- **New models blocked:** New foreign-made consumer-grade router models cannot receive FCC equipment authorization going forward.
- **Covered List status:** The FCC's Covered List now formally classifies foreign-made consumer routers alongside other prohibited communications equipment.
- FCC equipment authorization is required before any device can be imported, marketed, or sold in the US. Without it, new foreign-made models cannot legally enter the US market.

WHAT HAS NOT CHANGED

- **Existing devices:** Consumers and organizations may continue using any router they have already lawfully purchased or acquired. There is no recall, forced replacement, or usage restriction on existing hardware.
- **Previously authorized models:** Router models that previously received FCC equipment authorization remain authorized. They can continue to be imported, sold, and marketed.
- **Exemption pathway:** A Conditional Approval pathway exists. Manufacturers of foreign-made devices may apply to the Department of Homeland Security or the Department of War for exemption. Devices granted Conditional Approval remain eligible for FCC authorization.
- **Firmware and security updates:** Software and firmware updates to previously authorized devices are currently permitted. The FCC's Office of Engineering and Technology issued a blanket waiver on March 23 specifically to allow security patches and compatibility updates to already-authorized covered routers. The waiver runs until at least March 1, 2027. What happens after that date is unresolved and will depend on regulatory developments between now and then.

OPERATIONAL IMPLICATIONS FOR SECURITY AND IT TEAMS

- **No immediate action is required for devices currently deployed. Existing hardware is currently unaffected by this ruling (*see note on manufacturer firmware updates below*).**
- Procurement planning should account for reduced availability of new foreign-made consumer-grade router models over time as existing authorized inventory is consumed.
- Security teams reviewing supplier risk or third-party network infrastructure should note that the FCC determination formally validates router firmware integrity and supply chain provenance as material security concerns, consistent with NSA, CISA, and NCSC guidance issued in early 2025.
- Organizations relying on manufacturer firmware for security updates should note that the post-2027 update pathway for covered hardware is currently uncertain. Organizations using a managed firmware solution, where the firmware is maintained and updated independently of the hardware manufacturer, are structurally less exposed to this uncertainty.

W: loxada.com **T:** 617 586 1339 **E:** hello@loxada.com

- The Conditional Approval process (applications to conditional-approvals@fcc.gov) is the relevant pathway for organizations or vendors seeking to continue using foreign-made hardware not yet authorized under the new framework.

TECHNICAL CONTEXT

The FCC determination applies to consumer-grade routers, defined by device classification rather than end use. Organizations using consumer-grade hardware in commercial or enterprise deployments, a common pattern in hybrid and distributed work environments, fall within the scope of the ruling for procurement purposes.

The ruling does not address firmware integrity, management controls, or network isolation capabilities. A device's geographic origin is one supply chain risk factor. Others, including manufacturer firmware maintenance practices, vulnerability disclosure patterns, and the absence of centralized management and update controls, remain outside the scope of this determination and continue to represent structural security gaps regardless of where a device was manufactured.

> **Primary source:** *FCC Fact Sheet, March 23, 2026. All factual statements in this document are drawn directly from the FCC Fact Sheet (DOC-420034A1) and the accompanying Executive Branch determination. This document does not constitute legal or regulatory advice.*