

FCC Covered List Is Pushing Limits Of Supply Chain Scrutiny

By **Michael Huneke and Loyaan Egal** (October 6, 2026, 5:45 PM EDT)

The current administration is rapidly expanding the use of the Federal Communications Commission's covered list as a national security tool, extending restrictions beyond named companies and equipment to broad categories of foreign-produced connected equipment.

Companies well outside the traditional telecommunications sector may now need to consider FCC equipment authorization requirements as part of their supply chain and trade compliance programs, given recent additions covering uncrewed aircraft systems, consumer-grade routers, advanced robotic devices and power inverters.

The shift has potentially significant consequences. Equipment placed on the covered list generally cannot receive a new FCC equipment authorization. For devices that require authorization, that can effectively prevent future importation, marketing and sale in the U.S.

Recent actions also demonstrate that the government is increasingly looking beyond the identity of a manufacturer to where equipment is produced and, in some circumstances, what components are inside it.

Below, we examine the expansion of the covered list and identify practical considerations for companies managing the resulting supply chain and compliance risks.



Michael Huneke



Loyaan Egal

From Telecommunications Regulation to National Security Tool

Although it has worked closely with other agencies — e.g., the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, commonly referred to as "Team Telecom" — to address national security risk related to telecommunications authorizations and submarine cable licenses it grants and regulates, the FCC has not traditionally been viewed as a national security agency.

However, its authority over devices that emit radio frequency signals gives it an important role in regulating the connected equipment on which businesses and consumers increasingly rely.

In 2019, the Secure and Trusted Communications Networks Act of 2019, also known as the Secure Networks Act, established the covered list for communications equipment and services determined to pose an unacceptable risk to U.S. national security or the security and safety of U.S. persons. In 2021,

the Secure Equipment Act subsequently required the FCC to prohibit authorization of covered equipment.

Importantly, the FCC does not independently decide what belongs on the covered list. Under the Secure Networks Act, additions generally depend on determinations from specified national security agencies or interagency bodies — e.g., Team Telecom. Once the statutory requirements are satisfied, however, the FCC implements the resulting restrictions through its equipment authorization regime and uses its investigative and enforcement authorities to achieve compliance.

The covered list initially focused largely on equipment and services associated with specifically identified companies. More recent actions represent a significant expansion of that model.

In December 2025, the FCC relied on a national security determination made by a White House-convened executive branch interagency body to add uncrewed aircraft systems/drones and UAS critical components produced in foreign countries, subject to specified exceptions.

In March 2026, the FCC similarly relied on a White House-convened executive branch interagency body's national security determination to add consumer-grade routers produced in foreign countries, except those receiving conditional approval.

In July, foreign-produced advanced robotic devices and power inverters were added by relying again on the White House-led national security assessment process that was employed to include foreign-produced UAS/drones and consumer-grade routers to the covered list.

The national security rationale focuses in significant part on the risks created by connectivity. Connected devices can potentially provide avenues for remote access, surveillance, sensitive-data exfiltration, intellectual property theft, or disruption and sabotage. The government's consumer router determination, for example, cited the use of router vulnerabilities in major cyber campaigns, and warned that compromised devices could provide foreign actors a built-in backdoor to homes, businesses, critical infrastructure and emergency services.

Connected vehicles, which are being addressed separately by the U.S. Department of Commerce's information and communications technology and services supply chain authorities, pursuant to Executive Order No. 13873, illustrate the broader concerns. Modern vehicles contain communication, sensor, software and data collection technology.

Similar concerns can extend to other connected technologies that might provide surveillance capabilities near sensitive locations or enable remote interference with physical systems.

The New Model Looks Beyond Foreign Adversaries

Perhaps the most consequential feature of recent covered list actions is that they do not necessarily depend on whether equipment originates in a designated foreign adversary country.

The consumer router restriction, for example, applies to routers produced in a foreign country regardless of the producer's nationality. That means a U.S.-headquartered company's equipment could potentially fall within the restriction if the relevant production occurs abroad.

For companies accustomed to trade compliance frameworks centered on sanctioned jurisdictions,

restricted parties or countries of concern, this requires a different lens. A supply chain in Canada, Mexico, Europe or elsewhere may require analysis even where there is no traditional foreign-adversary connection.

The FCC is also moving deeper into products themselves. In July, the commission adopted rules prohibiting authorization of certain devices incorporating logic-bearing hardware components produced by entities identified on the covered list. The rule addresses components such as integrated circuits, modules and other hardware capable of processing or transmitting data, reflecting the concern that a compromised component can undermine an otherwise noncovered finished device.

The FCC has also sought comment on whether broader component-based restrictions are warranted.

The result is a regulatory model that increasingly demands visibility beyond Tier-1 suppliers.

Conditional Approvals Provide a Path for Some Foreign Production

The breadth of the new categorical restrictions has also produced a mechanism for distinguishing equipment that may not present the risks underlying the broader determination.

For certain categories, manufacturers can seek a conditional approval from designated national security agencies. For routers, for example, the FCC acts as the conduit for information reviewed by the U.S. Department of War and the U.S. Department of Homeland Security. A favorable determination allows specified equipment to remain outside the covered list restrictions for the approval period.

The process resembles a rebuttable presumption: Covered foreign production is presumed to present an unacceptable risk, but a company can provide information supporting a different determination for particular equipment.

The government's guidance as to the information required to request conditional approval illustrates the depth of the inquiry. Applicants must disclose corporate structure and ownership, including beneficial owners of 5% or more; board and executive leadership; and foreign government ownership or influence.

They must also provide detailed manufacturing and supply chain information, including a bill of materials, component countries of origin, software and intellectual property ownership and responsibilities, and potential supply chain choke points.

The government also seeks information concerning plans to establish trusted manufacturing capacity in the U.S.

Conditional approvals have already been granted for certain UAS/drones and consumer router products, demonstrating that the process is not merely theoretical. The conditional approvals that have been granted have varied in length, with no end dates assigned to UAS/drones and various dates assigned to consumer routers.

What Companies Should Do Now

For businesses that manufacture, import, integrate, distribute or rely on connected equipment, covered list compliance is becoming a supply chain exercise as much as an FCC exercise.

Companies should consider:

- Mapping products and components against current covered list categories: Determine which products and components may fall within existing categories and which products require FCC authorization;
- Reviewing the supply chain beyond tier-one suppliers: Identify where equipment and potentially relevant components are produced, who supplies them, and whether supplier representations remain reliable when sourcing, manufacturing locations or component suppliers change.
- Maintaining detailed documentation: Keep records of supplier inquiries, equipment authorizations, countries of production, bills of materials where appropriate and the level of diligence applied to particular suppliers.
- Tracking authorization dates and product changes: Existing equipment authorizations may receive different treatment from future authorizations, therefore companies should document authorization dates and monitor subsequent software, firmware, hardware and component changes.
- Monitoring adjacent sectors: The rapid progression from drones to routers, robotics and power equipment suggests that the covered list is becoming an increasingly important tool for addressing risk in the information and communications technology and services supply chain. Companies should monitor developments affecting sectors adjacent to those already covered.
- Assessing embedded components: Recent FCC action on logic-bearing hardware components reinforces the need to understand what is inside connected products. As connected functionality becomes embedded in more products, the distinction between a telecommunications company and a company subject to telecommunications regulation is becoming less useful.
- Preparing to conduct risk-based due diligence: When any addition to the covered list potentially impacts a company's path to market, the company should be prepared to conduct risk-based due diligence on proposed alternative suppliers or other alternative counterparties. This will help the company mitigate the risk of later investigations or enforcement actions by the FCC, or other U.S. government agencies, regarding whether new counterparties are indeed bona fide or, instead, are suspected of participating in a scheme to evade the covered list's restrictions.

The practical challenge is not simply determining whether a company appears on a government list. Increasingly, companies may need to know what is inside their products, where those products and components were made, who controls the relevant technology, and how those facts can be documented if regulators come asking.

Developments that have been building for years can move quickly once they reach a tipping point. For companies with globally distributed manufacturing and connected products, understanding the supply chain before the next covered list expansion may be considerably easier than reconstructing it afterward.

Michael Huneke is a partner at Morgan Lewis & Bockius LLP.

Loyaan Egal is a partner at Morgan Lewis. He previously held several positions at the FCC, including as chief of the FCC Enforcement Bureau. He also served on the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector and as a deputy chief of the Foreign Investment Review Section of DOJ's National Security Division.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.