Federal Communications Commission

Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program

47 CFR Part 2

[ET Docket No. 21-232; FCC 25-71; FR ID 318981]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Annie Fixler
Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation

Washington, DC
December 23, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chinese equipment continues to pose both an espionage and a sabotage threat to U.S. networks. Over the course of the past half-decade, Beijing has become more aggressive in targeting American critical infrastructure, including health care networks, utilities, and telecommunications, both to collect intelligence and to potentially introduce vulnerabilities that may be exploited in the event of a crisis with the United States. These efforts have followed in parallel with China's cyber operations targeting the federal government, the American military, and defense contractors, each of which may have provided exquisite intelligence or hindered Washington's capacity to deter or defeat Beijing if necessary.

While the Federal Communications Commission (FCC) has been proactive in protecting the United States from the threats posed by equipment produced by entities on the commission's Covered List, these firms maintain a presence in the American market due to their integration into long-standing supply chains and their deployment across a range of critical sectors. Despite the FCC's previous actions, thousands of authorized devices, which no longer meet the Commission's criteria, remain installed across the country.

To close these gaps and combat this threat, the FCC should adopt a more comprehensive set of regulations to remove equipment produced by entities on the Covered List from U.S. networks and infrastructure while encouraging American service providers to switch to alternative components produced by U.S. allies and partners.

Recommendations:

- **The Commission should require that any authorized device that is modified by an entity identified on the Covered List be recertified.** To maintain a single procedure for all equipment authorization applications proposed by an entity on the Covered List, the FCC should require all equipment modified by these entities to undergo the full certification process. This oversight would prevent any entity currently on the Covered List from modifying previously authorized equipment in ways that might introduce new vulnerabilities following purchase or installation. This move will likely also encourage American firms to transition toward alternate suppliers, further bolstering U.S. national security.

- **The Commission should prohibit the authorization of any equipment that contains any components produced by Covered entities**. Rather than attempt to pinpoint specific components that may harbor vulnerabilities, such as modular transmitters, logic-bearing hardware, firmware, software, or semiconductors, the FCC should enact the

broadest possible prohibitions to safeguard U.S. national security. This move will have the secondary benefit of incentivizing American firms to phase out all covered equipment due to concerns over potential supply chain-related shocks following any possible further rule-making activity.

- **The Commission should adopt the definition of "critical infrastructure" based on the USA PATRIOT ACT (Public Law 107-5).** The FCC should adopt the following definition of critical infrastructure: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or a combination of those matters." This definition has been used in numerous national security documents since its passage and is functionally similar to other definitions used across the federal government, particularly by the Department of Homeland Security. At the same time, the FCC should also consider how this definition will apply to distributed systems, which in the aggregate may serve as critical infrastructure, such as local broadcast networks.

- **The Commission should strengthen enforcement of marketing prohibitions to prevent unauthorized equipment from entering the supply chain.** The Commission should consider requiring periodic verifications of the authorization status of imported inventory to ensure that the equipment, which may have entered the country prior to the imposition of new restrictions, remains compliant with FCC standards. This move, while generating upfront costs for businesses, will eventually be a cost-saving measure by preventing the need for consumers to either replace vulnerable products following final sales or from suffering the consequences of a potential defect.

Conclusion

By strengthening layered supply chain accountability, the Commission can bolster U.S. national security while supporting continued innovation in the telecommunications industry. The cost of inaction — measured in both dollars and national security risk — grows every day, signaling to adversaries that regulatory loopholes can be exploited to maintain access to U.S. critical infrastructure.

Thank you for considering our comments, and we look forward to seeing how our input is incorporated into the Commission's ongoing policy work.