GAO Highlights

TELECOMMUNICATIONS

Selected Agencies Have Taken Steps to Address Risks of Equipment Linked to China

GAO-26-107668 May 2026

A report to congressional requesters

Contact: Andrew Von Ah at vonaha@gao.gov or Jennifer Franks at franksj@gao.gov.

What GAO Found

A 2018 law generally prohibits executive agencies from procuring telecommunications and video surveillance equipment produced by certain companies, or their subsidiaries and affiliates, linked to the People's Republic of China (referred to as "covered equipment"). Agencies are not prohibited from using covered equipment procured prior to this prohibition. Officials from four of six selected agencies—the Departments of Homeland Security, Justice, State, and Treasury—told GAO they did not identify any covered equipment connected to their IT networks. The Departments of Defense (DOD) and Energy reported finding little covered equipment in recent searches and having efforts underway to address potential risks. For example, DOD officials identified three instances of covered equipment connected to its network and confirmed the devices have been blocked from external access while DOD acts to remove them.

All six selected agencies have used a combination of methods to search for covered equipment since 2019. Each method has benefits and limitations. For example, IT network scans may not scan agencies' entire IT networks, including classified networks.

Methods Selected Agencies Have Used to Search for Covered Equipment, 2019–December 2025

Agency	IT hardware asset inventory search[a]	IT network scan[b]	Procurement record search	Physical search
Department of Defense	X	X	–	X
Department of Energy	X	X	–	–
Department of Homeland Security	X	X	X	–
Department of Justice	X	X	X	–
Department of State	X	X	–	–
Department of the Treasury	X	X	X	–

Source: GAO analysis of agency responses. | GAO-26-107668

Note: "Covered equipment" refers to "covered telecommunications equipment" as defined by the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3), 132 Stat. 1636, 1918 (2018).

[a]IT hardware asset inventories are records of IT hardware assets owned by an agency.
[b]IT network scans use software to identify devices active on an IT network.

Officials at some of the selected agencies cited limited visibility into product supply chains as a challenge in identifying covered equipment. For example, one agency official noted that manufacturers were reluctant to share proprietary information about their supply chains, thereby limiting the agency's ability to determine whether devices in its inventory contained components produced by covered entities. Some officials said the lack of comprehensive, authoritative information on companies' subsidiaries and affiliates also posed a challenge. However, officials noted that such information would be accurate only at the time it was developed, because companies may change their names or acquire or divest subsidiaries and affiliates.

Why GAO Did This Study

The federal government depends on a complex network of telecommunications and video surveillance equipment to support operations and communicate with the public. Foreign adversaries may seek to exploit vulnerabilities in this equipment. According to the Office of the Director of National Intelligence, China poses the most active and persistent cyber threat to the federal government.

GAO was asked to review issues related to federal agencies' use of covered equipment. This report examines (1) the amount of covered equipment selected agencies have identified, and actions the agencies have taken to address risks associated with using the equipment; and (2) the methods selected agencies reported using to search for covered equipment and challenges they have experienced.

To conduct this review, GAO selected the six agencies from the Chief Financial Officers Act of 1990 that have organizational entities in the Intelligence Community. GAO obtained and reviewed information (e.g., screenshots of network scans or inventory searches) on selected agencies' identification of covered equipment, if any, and actions to address associated risks.

GAO also reviewed agencies' policies and procedures for developing and maintaining inventories of hardware assets (i.e., equipment) and compared them with relevant National Institute of Standards and Technology cybersecurity requirements. Further, GAO reviewed documentation and interviewed agency officials about their methods for searching for covered equipment and the challenges they faced in identifying the equipment.