United States Government Accountability Office

Report to Congressional Requesters

May 2026

TELECOMMUNICATIONS

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

GAO-26-107668

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.

Contents

Letter 1

Background 4
Selected Agencies Identified Little or No Covered Equipment in Recent Searches and Are Taking Steps to Address Risks 8
Agencies Used Various Methods to Search for Covered Equipment but Cited Challenges in Identifying It 12
Agency Comments 18

Appendix I GAO Contacts and Staff Acknowledgments 19

Table

Table 1: Methods Selected Agencies Reported Using to Search for Covered Equipment, 2019–December 2025 13

Figures

Figure 1: Example of How a Cybersecurity Threat Actor Could Access and Exploit an IT Network 5
Figure 2: Description of the Methods Selected Federal Agencies Have Used to Identify Devices 14

Abbreviations

CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
DCDC	Department of Defense Cyber Defense Command
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
FISMA	Federal Information Security Modernization Act
NIST	National Institute of Standards and Technology
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OUSD (I&S)	Office of the Undersecretary of Defense for Intelligence and Security
PRC	People's Republic of China

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 19, 2026

The Honorable James Comer
Chairman
Committee on Oversight and Government Reform
House of Representatives

The Honorable Ashley Hinson
House of Representatives

The federal government depends on a complex and expansive network of telecommunications and video surveillance equipment to support its operations and disseminate information to the public. Federal agencies are vulnerable to cyber threats from foreign adversaries that may seek to exploit weaknesses in this equipment.

In August 2024, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) warned that cameras manufactured by a company linked to the People's Republic of China (PRC) had critical vulnerabilities that malicious threat actors had exploited. In addition, since at least 2021, PRC-linked threat actor Volt Typhoon has infiltrated U.S. telecommunications and critical infrastructure sectors. These actions compromised sensitive telecommunications systems, exposed vulnerabilities, and exfiltrated data from telecommunications, energy, transportation, and water systems.[1] According to the Office of the Director of National Intelligence's (ODNI) 2026 Annual Threat Assessment, the PRC continues to pose the most active and persistent cyber threat to the U.S. government.[2] Due to ongoing concerns such as these, cybersecurity has been on our High-Risk List since 1997.[3]

[1]Under the Critical Infrastructures Protection Act of 2001, "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. Pub. L. No. 107-56, § 1016(e), 115 Stat. 400, 401 (codified at 42 U.S.C. § 5195c(e)).

[2]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 14, 2026).

[3]For the most recent update, see GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

Section 889 of the National Defense Authorization Act for Fiscal Year 2019 addresses certain threats posed by the PRC.[4] Section 889 generally prohibits executive agencies from procuring covered equipment or services—that is, telecommunications and video surveillance equipment and services produced or provided by certain PRC-linked companies or their subsidiaries or affiliates.[5] For this report, we refer to certain PRC-linked companies or their subsidiaries or affiliates as "covered entities." The PRC-linked companies include Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company. Section 889 authorizes waivers of this prohibition if the Director of National Intelligence determines a waiver is in the national security interests of the U.S.[6] Further, Section 889 does not prohibit agencies from using covered equipment or services that were procured before the procurement prohibition took effect. As a result, federal agencies may continue to use covered equipment or services that pose a risk to the U.S. government.

You asked us to review issues related to federal agencies' use of covered equipment.[7] This report examines (1) the amount of covered equipment

[4]John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917–19 (2018).

[5]The term "covered equipment and services" includes (1) telecommunications equipment produced by Huawei Technologies Company, ZTE Corporation, or their subsidiaries or affiliates; (2) telecommunications and video surveillance equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or their subsidiaries or affiliates; (3) telecommunications or video surveillance services provided by such entities or using such equipment; and (4) telecommunications and video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with specified officials, reasonably believes is connected to the government of the People's Republic of China. *Id.* § 889(f)(3). Subject to waivers, the prohibition applies if the equipment or service is used "as a substantial or essential component of any system, or as critical technology as part of any system." *Id.* § 889(a)(1). The Federal Acquisition Regulation defines "substantial or essential component" to mean "any component necessary for the proper function or performance of a piece of equipment, system, or service" and cites other statutes and regulations for lists of items considered to be "critical technology." 48 C.F.R. § 4.2101. This report also uses the term "covered device" to refer to an individual piece of covered equipment.

[6]Section 889 also allowed heads of executive agencies to grant one-time waivers that would be effective no longer than through August 13, 2021, for these requirements. Pub. L. No. 115-232, § 889(d), 132 Stat. at 1918.

[7]You also asked us to review issues related to federal agencies' use of covered services. We did not focus our work on covered services, because most service contracts for covered equipment procured prior to Section 889's effective date have likely expired, reducing the likelihood that federal agencies are still using these covered services.

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 the challenges they have experienced in identifying this equipment.

To conduct this review, we selected the six agencies from the Chief Financial Officers Act of 1990 that have organizational entities in the Intelligence Community—the Department of Defense (DOD), Department of Energy (DOE), DHS, Department of Justice (DOJ), Department of State, and Department of the Treasury.

To examine the amount of covered equipment the selected agencies have identified and actions they have taken to address associated risks, we reviewed documents (e.g., policies and guidance) and interviewed officials. We obtained information from the selected agencies about covered equipment connected to their IT networks (e.g., routers and modems), as well as covered equipment not connected to their IT networks (e.g., cell phones). We asked selected agencies about the amount of covered equipment they identified through any of the searches they conducted from 2019, the year Section 889's procurement prohibition took effect, through August 2025, when we completed the evidence-gathering phase of our work.

To provide more recent information in our report, in September 2025, we requested that the selected agencies provide us with more recent results of department-wide network scans or results of IT hardware inventory searches for covered equipment.[8] The agencies scanned their networks or searched their IT hardware asset inventories on a single day at different points in time from September 2025 through December 2025. We reviewed screenshots showing how the scans or searches were configured, as well as the detailed output showing the results.

To examine the methods selected agencies reported using to search for covered equipment since 2019 and the challenges they faced, we reviewed agencies' policies and procedures and interviewed officials. We compared agencies' policies and procedures for one method for searching for covered equipment—specifically, developing and maintaining their inventories of hardware assets (i.e., equipment)—with

[8]Specifically, we asked selected agencies to scan or search for all covered entities. We did not ask the agencies to scan or search for subsidiaries or affiliates of the covered entities because, as we note later in the report, there is no authoritative, comprehensive list of subsidiaries or affiliates that is publicly available and disseminated.

relevant cybersecurity requirements from the National Institute of Standards and Technology (NIST). We reviewed screenshots of agencies' IT hardware asset inventories, which specified the types of data gathered for each piece of equipment (e.g., manufacturer, model, and location). We focused on agencies' development and maintenance of hardware asset inventories because, per NIST requirements, the inventories should contain information on equipment manufacturers, which could be used to search for covered equipment. We also interviewed agency officials about their search methods and the challenges they faced in identifying covered equipment.

We conducted this performance audit from June 2024 to May 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

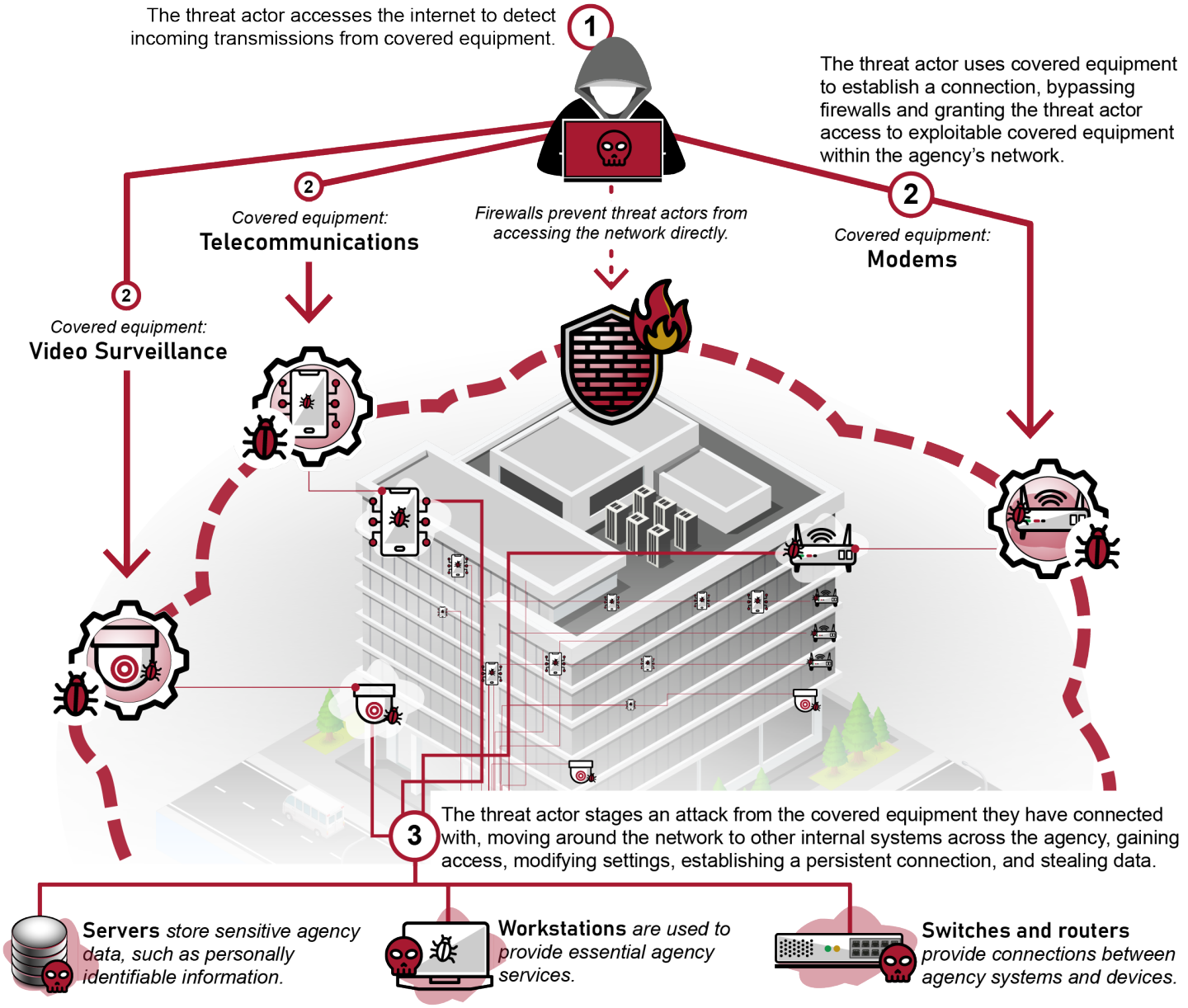
Cybersecurity Risks of Telecommunications and Video Surveillance Equipment Manufactured by Covered Entities

As we previously reported, federal agencies can face cybersecurity risks from using telecommunications and video surveillance equipment manufactured by covered entities.[9] These risks are heightened when such equipment is connected to an agency's IT network, as the equipment can then be exploited remotely by malicious threat actors. PRC-linked threat actors may use internet-based access to infiltrate the equipment, enabling them to penetrate deeper into the agency's IT environment. This access can facilitate the spread of malware, compromise sensitive information and essential services, and potentially enable large-scale cyberattacks across government systems.[10] See figure 1 for an example of how telecommunications or video surveillance equipment may be integrated into an agency's IT network, and how threat actors could exploit this connectivity.

[9]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

[10]Malware is any software used to gain unauthorized access to IT systems in order to steal data, disrupt system services, or damage IT networks in any way.

Figure 1: Example of How a Cybersecurity Threat Actor Could Access and Exploit an IT Network



Sources: GAO analysis of cyber threat information (data); GAO (hacker, server, and switch icons); syafak/stock.adobe.com (building); Uniconlabs/stock.adobe.com (all other icons). | 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). Covered equipment is telecommunications and video surveillance equipment produced by certain companies linked to the People's Republic of China or by their subsidiaries or affiliates.

Equipment that is not connected to the agencies' IT networks, such as cell phones, can still pose a risk if such equipment uses other external networks, such as cellular networks, that could be subject to exploitation. These devices can be exploited by threat actors who target the external networks or the equipment themselves, potentially leading to credential theft, data compromise, or unauthorized access once the device interacts with agency resources. For example, according to CISA, PRC-affiliated actors have been observed compromising telecommunications and private communications of individuals involved in government or political activities.

Federal Standards and Guidance on Agencies' IT Hardware Asset Inventories

Civilian agencies and DOD have established federal information security standards and guidelines for agencies to develop an inventory of IT hardware assets, including telecommunications and video surveillance equipment. These standards and guidance include but are not limited to the following:

- **NIST security standards and guidelines.** NIST SP 800-53: *Security and Privacy Controls for Information Systems and Organizations* provides a catalog of security and privacy controls for federal organizational operations, including requirements for developing and maintaining IT hardware asset inventories.[11] Specifically, NIST SP 800-53 requires agencies to develop and maintain an inventory that reflects the current state of the information system and includes necessary details—such as manufacturer, model, and physical location—for effective tracking and reporting. The Federal Information Security Modernization Act of 2014 (FISMA)[12] generally requires

[11]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: December 2020).

[12]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073, largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946. As used in this report, FISMA refers both to FISMA 2014, as amended, and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

agencies to comply with certain NIST information security standards.[13]

- **Office of Management and Budget (OMB) Memorandum: *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*.** This memorandum provides specific guidance and deadlines for agencies to implement Zero Trust Architecture.[14] Zero Trust Architecture is a cybersecurity framework that assumes that threats can exist both inside and outside an organization's network, so no user, device, or system is automatically given access. According to OMB, Zero Trust Architecture necessitates that entities have ongoing, reliable, and complete asset inventories.
- **OMB Memorandum: *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.** This memorandum requires that civilian agencies, to the maximum extent feasible, automate reporting on IT hardware assets through the Continuous Diagnostics and Mitigation (CDM) program.[15] DHS developed the CDM program in 2012 to strengthen the cybersecurity of government networks and systems by providing tools to agencies to support continuous monitoring of their networks.[16] As we previously reported, the asset management program area of CDM, if implemented effectively, should enable agencies to create ongoing,

[13]NIST SP 800-53 states that its information standards and guidelines do not apply to national security systems without the express approval of the appropriate federal officials exercising authority over such systems. The Committee on National Security Systems has adopted NIST SP 800-53, as documented with some distinctions in its Instruction No. 1253, for the national security community. Committee on National Security Systems, *Categorization and Control Selection for National Security Systems,* Instruction No.1253 (July 29, 2022).

[14]Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, OMB Memorandum M-22-09 (Washington, D.C.: Jan. 26, 2022).

[15]This memorandum states, "Agencies are required to report at least 90 percent of Government-furnished equipment (GFE) through the CDM program… Agencies must continue to provide data on assets in an automated manner to the maximum extent feasible. This is supported by the adoption throughout each agency of CDM and other technical solutions that provide visibility and automated reporting directly to CISA." Office of Management and Budget, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements,* OMB Memorandum M-25-04 (Washington, D.C.: Jan. 15, 2025).

[16]CISA requires executive, civilian agencies to automate asset discovery every 7 days and vulnerability scans every 14 days, and to upload vulnerability results to the CDM dashboard generally within 72 hours of completion. Cybersecurity and Infrastructure Security Agency, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, Binding Operational Directive 23-01 (2023).

reliable, and complete asset inventories and should support agency implementation of Zero Trust Architecture.[17]

- **DOD's Zero Trust Strategy.** DOD's Zero Trust Strategy emphasizes the need for visibility and control over all devices that access DOD's IT network.[18] As part of that strategy, DOD implemented the Comply-to-Connect framework department-wide to help it transition to a Zero Trust Architecture by the end of fiscal year 2027. The Comply-to Connect framework contains tools and techniques that help DOD's components identify all equipment connected to the IT network. DOD officials said they require components to report this information to its Continuous Monitoring and Risk Scoring application.[19]

Selected Agencies Identified Little or No Covered Equipment in Recent Searches and Are Taking Steps to Address Risks

Four Agencies Found No Covered Equipment Connected to Their IT Networks, and the Two That Did So Have Efforts to Address Risks

Four of the six selected agencies—DHS, DOJ, State, and Treasury—reported to us that their searches from 2019 through August 2025, as well as more recent searches they conducted in response to our September 2025 request, found no covered equipment connected to their IT

[17]GAO, *Cybersecurity: Network Monitoring Program Needs Further Guidance and Actions*, GAO-25-107470 (Washington, D.C.: June 11, 2025).

[18]DOD, *DOD Zero Trust Strategy* (October 2022).

[19]The Continuous Monitoring and Risk Scoring application is a suite of software solutions used by DOD to monitor the cybersecurity posture of DOD's information systems on a continual basis and support risk-based decision-making and vulnerability management. According to the Continuous Monitoring and Risk Scoring program management office, nearly all of DOD's components submit data to the application.

networks.[20] DOD and DOE reported finding a few covered devices in recent searches, and they had both identified covered devices in prior searches. Both agencies have undertaken efforts to address potential risks posed by this equipment.

DOD. DOD reported finding covered equipment connected to its networks in a recent search. Specifically, in response to our request, DOD's Cyber Defense Command (DCDC) conducted a network scan in December 2025 for covered equipment and identified three covered devices connected to DOD's IT network.[21] DCDC officials said they confirmed that the devices have been blocked from external access while DOD takes steps to remove them.[22]

In addition, DOD previously identified other covered equipment connected to its IT network. Specifically, in 2019 the Office of the Undersecretary of Defense for Intelligence and Security (OUSD (I&S)) worked with DOD components to inventory the models, locations, and quantities of covered video surveillance equipment, such as cameras and recorders, in use at DOD facilities. Through this inventory, DOD components identified more than 300 video surveillance devices connected to DOD's IT network that were manufactured by one of the five PRC-linked entities listed in Section

[20]The focus of our review is on telecommunication and video surveillance equipment (i.e., hardware) manufactured by covered entities, not software produced by those entities. Nonetheless, in response to our request to search for covered equipment, DHS identified software developed by covered entities on DHS's network. The officials stated that they removed the software from their network and confirmed its removal through follow-up searches.

[21]DOD's IT network comprises 45 geographically and functionally defined areas of operation. Each area of operation has a designated component commander or director who is responsible for securing, operating, and defending their area of DOD's IT network. DCDC is a U.S. Cyber Command component responsible for coordinating with the designated component commander or directors to conduct DOD-wide defensive cyber operations.

[22]DCDC officials said that DCDC's network scan covered the perimeter of DOD's IT network. DCDC can review network scanning results and information from the Continuous Monitoring and Risk Scoring application dashboard to identify threats, such as covered equipment connected to the areas of DOD's IT network operated by DOD components.

889.[23] DOD determined that over 40 percent of this equipment posed a high risk, because it was located in secure spaces.[24] An OUSD (I&S) official stated that from March through May 2021, OUSD (I&S) held discussions with DOD and DOD component Chief Information Offices to develop plans to mitigate the risks of this covered equipment. At that time, DOD took no further action due to a lack of consensus on what steps to take.

More recently, however, DOD has taken actions to address potential risks of any remaining covered equipment. Specifically, as part of Comply-to-Connect, DOD components must identify all devices connected to the IT network; these devices would include any covered video surveillance equipment still being used. DOD components must also determine whether the devices comply with DOD's cybersecurity standards, which require devices to have the appropriate anti-malware, firewall, and other vulnerability management software. According to the DOD Chief Information Office, DOD components must achieve full operational capability of Comply-to-Connect by September 30, 2026.[25]

DOE. In December 2025, in response to our request, DOE scanned its network and found one potential instance of covered equipment in use in one of its program offices. DOE officials told us that the scan may have incorrectly identified the equipment as covered equipment, and that they were researching the validity of the scan results. DOE officials told us that if they determine the equipment is covered equipment, then they will remove the equipment or take other actions, as appropriate. In addition, DOE officials said that previous searches in 2019 had identified some covered equipment, which they subsequently removed.

[23]In addition to identifying video surveillance equipment manufactured by the five PRC-linked entities identified in Section 889, OUSD (I&S) instructed DOD components to identify 1) equipment manufactured by any entity on OUSD (I&S)'s list of subsidiaries and affiliates of those entities, as well as 2) any video surveillance equipment manufactured by several entities that disclosed that one or more of their products or product lines qualify as covered equipment under the statute. In total, DOD identified about 1,500 covered video surveillance devices connected to DOD's IT network.

[24]For the purposes of DOD's search, secure space means any space to which access has been restricted for national security reasons or limited to official business only, including government workspace (if the space contains classified information) and critical infrastructure and operational facilities.

[25]In January 2025, the DOD Inspector General initiated a review to assess the effectiveness of DOD's implementation of the Comply-to-Connect requirements.

Three Agencies Reported Using Some Covered Equipment Not Connected to Their IT Networks and Addressing Associated Risks

Equipment that is not connected to an agency's IT network can still present cybersecurity risks. For example, such equipment may transmit or receive data over external commercial or wireless networks that are outside the agency's security monitoring and control. Three of the six selected agencies—DOD, DOJ, and Treasury—reported using some covered equipment (e.g., stand-alone video surveillance cameras or cell phones) that was not connected to their IT networks. Officials said the agencies were taking actions to address associated risks.[26]

DOD. DOD's 2019 video surveillance inventory found more than 1,000 video surveillance devices not connected to DOD's IT network that were manufactured by one of the five PRC-linked entities listed in Section 889.[27] DOD considered this video surveillance equipment to pose either moderate or significant risks, based on whether the equipment was in a public or secure space.[28] In August 2025, officials from OUSD (I&S) and the DOD Chief Information Office told us that they did not know whether this equipment was still in use. However, an OUSD (I&S) official said that most of this equipment had likely been replaced, because DOD typically replaces video surveillance equipment when the warranty expires. The official also stated that many of the covered video surveillance devices identified in this inventory were in outdoor environments and, as a result, would have an average lifespan of approximately 5 years. Further, the official noted that the prohibition on covered services in Section 889 prohibits components from renewing service contracts to repair or replace this equipment. As a result, DOD likely no longer has the devices it identified in 2019.

DOJ. DOJ officials said the agency uses covered equipment to support its missions in countries where such devices are the only ones compatible with the telecommunications networks in those countries. The officials said that they have waivers from ODNI to procure the equipment, and that

[26]For DOJ and Treasury, we cannot report on the specific amount of covered equipment not connected to the agencies' IT networks, because details about the equipment are sensitive or are not public record.

[27]These are video surveillance devices that only connect to stand-alone networks that have no connection to DOD's broader IT network.

[28]OUSD (I&S) designated stand-alone video surveillance equipment in public spaces as a moderate risk, and stand-alone video surveillance equipment in secure spaces as a significant risk. The office designated networked video surveillance equipment in public spaces as a significant risk, and as noted previously, designated networked video surveillance equipment in secure spaces as high risk.

they coordinate with ODNI on risk mitigation practices.[29] For example, DOJ officials said DOJ has a memorandum with ODNI describing risk mitigation controls for the covered cell phones procured under the waiver. DOJ officials also stated that DOJ prohibits agents from connecting to its IT networks using these devices and instructs them to avoid discussing sensitive operations using this equipment.

Treasury. In December 2025, Treasury officials reported that the agency used covered equipment not connected to its IT networks—specifically, analog cameras—in one facility, and we found that Treasury was in the process of acquiring equipment to replace it.

Agencies Used Various Methods to Search for Covered Equipment but Cited Challenges in Identifying It

Agencies Have Searched for Covered Equipment Using Asset Inventory Searches, IT Network Scans, and Other Methods

Officials at the six selected agencies told us that they have used various methods to search for covered equipment since 2019 (see table 1). In addition, five of the six selected agencies reported using automated tools to continuously monitor their networks to maintain ongoing visibility into their security posture.

[29]ODNI may waive Section 889's prohibitions if the Director of National Intelligence determines the waiver is in the national security interests of the U.S. Pub. L. No. 115-232, § 889(d)(2), 132 Stat. at 1918.

Table 1: Methods Selected Agencies Reported Using 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	-

Legend: "X" = indicates method used "—" = indicates that the method was not used

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

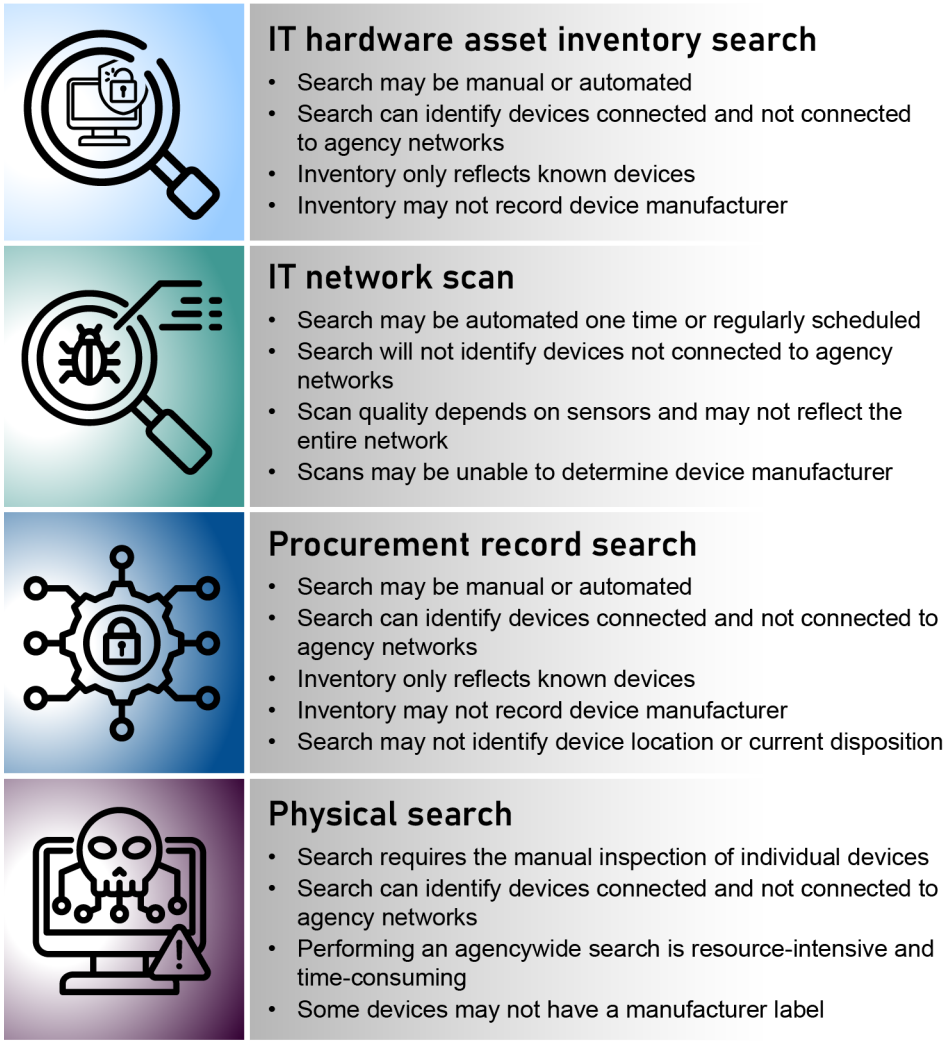
Note: "Covered equipment" refers to "covered telecommunications equipment" as defined by the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3), 132 Stat. 1636, 1918 (2018). Covered equipment is telecommunications and video surveillance equipment produced by certain companies linked to the People's Republic of China or by their subsidiaries or affiliates.

[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.

Each of the methods that agencies used to search for covered equipment has benefits and limitations. For example, by running an automated IT network scan, agencies can identify covered equipment connected to their IT networks but cannot identify equipment that is not connected. In addition, IT network scans depend on the placement of sensors on the equipment and may not reflect the entire network, including classified networks and equipment that connects to their enterprise networks intermittently (e.g., cell phones). Procurement record searches and physical searches enable agencies to identify equipment that is connected to their IT networks as well as equipment that is not connected. However, procurement records may not provide agencies with information on where the devices are located, and physical searches are resource-intensive and time-consuming. See figure 2 for a description of each search method.

Figure 2: Description of the Methods Selected Federal Agencies Have Used to Identify Devices



Sources: GAO analysis of agencies' search methods; Uniconlabs/stock.adobe.com (all icons). | GAO-26-107668

IT hardware asset inventory searches. All six selected agencies searched their IT hardware asset inventories to identify covered equipment. As discussed above, NIST requires agencies to develop and document an IT hardware asset inventory that includes the names of the asset manufacturers. Based on our review of screenshots provided by the agencies, we found that all six agencies have developed IT hardware

asset inventories.[30] For example, DOJ officials said that DOJ queried its CDM program dashboard to obtain an authoritative inventory of IT hardware and software assets across the agency, which it uses in conjunction with another tool to automatically screen for covered equipment. In addition to serving as an inventory, the CDM program provides tools to agencies to enable continuous monitoring of their networks.

IT network scans. Officials at all six agencies said they had conducted network scans to identify covered equipment connected to their IT networks.[31] For example, officials at DCDC said they assess the results of DOD components' network scans and information from the departments' Continuous Monitoring and Risk Scoring application dashboard to identify cybersecurity threats, such as covered equipment. The officials said DCDC issued directives to the Army and Navy after it discovered covered equipment, such as routers, on the components' networks using these methods.

Procurement record searches. Officials at three of the six agencies—DHS, DOJ, and Treasury—stated that their agency reviewed procurement records to search for covered equipment. By reviewing procurement records, agencies can identify covered equipment regardless of whether it is connected to their network. For example, DOJ officials said that DOJ supplemented its network scans with a review of acquisition-related risk assessments.[32] DHS and Treasury officials said they also reviewed their agencies' procurement information to help search for covered equipment.

Physical searches. One agency—DOD—provided documentation on physical inspections it conducted to identify covered video surveillance equipment as part of a department-wide search. Physical inspections are a means of searching for equipment that may not be identified in network scans. According to an OUSD (I&S) official, in many cases, components'

[30]In some cases, agencies identified a single system as their IT hardware asset inventory of record, while officials at other agencies stated that multiple inventories served this function.

[31]Most selected agencies reported that their network scans encompassed 76 percent to 100 percent of total network equipment. According to officials, the scans may not capture the entire network because of their classified networks, and because some devices connect to the network intermittently (e.g., mobile devices).

[32]According to DOJ, its Supply Chain Risk Management Program conducts risk assessments to identify threats associated with vendors, including evaluations to determine whether suppliers have potential connections to the PRC.

facilities or logistics staff visually inspected cameras and recording devices to determine whether the devices were covered equipment.[33]

In addition to using the methods described above to search for covered equipment, five of the six agencies said they have used certain technologies to ensure they immediately identify any such devices attempting to connect to their IT network and take appropriate actions.[34] These technologies include network access control and endpoint protection. For example, Treasury requires its bureaus to automatically detect unauthorized devices, isolate them, and disable their network access. Additionally, DCDC officials said they search DOD's IT network for covered equipment in ongoing cyber operations and use cybersecurity tools to detect and block covered equipment on a monthly basis.

Agencies Cited Limited Visibility into Product Supply Chains and Other Challenges in Identifying Covered Equipment

Officials at the selected agencies described limited visibility into product supply chains; rebranding and sale of equipment by other companies; and the lack of comprehensive, authoritative information on subsidiaries and affiliates as challenges in identifying covered equipment.

Limited visibility into product supply chains. Officials from some selected agencies said that limited visibility into product supply chains was a key challenge to identifying covered equipment. For example, officials from State said telecommunications equipment it had procured from resellers prior to Section 889's enactment could include covered equipment or components, as there was no requirement for resellers to disclose whether they were sourcing products or components from covered entities.[35] DHS officials noted that manufacturers were reluctant

[33]According to OUSD (I&S), 17 of the 46 DOD components participated in this inventory. The nonparticipating components were nearly all tenants in other participating components' buildings or received security services provided by another participating component. OUSD (I&S) estimated the responding components were responsible for more than 75 percent of DOD's spaces where covered video surveillance equipment would likely be located.

[34]Officials at the remaining agency said that the technologies that the agency's sites and components use to detect and respond to attempts to connect covered devices to the IT network may vary. The officials said that they have not yet identified and addressed potential gaps in network access control across the agency, but that some sites and components may control access to the network using their own technologies. In addition, the officials told us that their agency has deployed endpoint protection tools in most of its sites and components, and that the remaining sites and components have deployed other endpoint protection tools, as appropriate.

[35]Subsequent to Section 889's enactment, the Federal Acquisition Regulation was amended to require contract offerors to represent whether the offered products or services include covered equipment. 48 C.F.R. § 52.204-26.

to share sensitive or proprietary information about their supply chains, thereby limiting DHS's ability to determine whether devices in its existing inventories contained components manufactured by subsidiaries or affiliates of the Section 889 companies.

Rebranding and sale of equipment by other companies. "White-labeling"—when equipment, such as telecommunications and video surveillance equipment, is rebranded and sold by a company other than the manufacturer—also poses a challenge to identifying covered equipment. This practice makes it difficult to identify the manufacturer of these devices and may undermine legal requirements like the Section 889 prohibition. For example, Treasury officials said the agency became aware of covered video surveillance equipment in use at its facilities through a multiagency investigation into a U.S. company that colluded with a covered entity to sell white-labeled equipment to Treasury under false pretenses.[36]

Lack of comprehensive, authoritative information on subsidiaries and affiliates. Officials from some selected agencies cited the lack of comprehensive, authoritative information on subsidiaries and affiliates of the five covered entities listed in Section 889 as a challenge to identifying all covered equipment. For example, DHS officials said that not having such information makes it difficult to identify all covered equipment. In prior work, we have reported on national security and other risks associated with undisclosed ownership and control of companies, including subsidiaries and affiliates, engaged in business with the federal government.[37] Officials noted, however, that any such information on subsidiaries and affiliates could quickly become outdated, because companies may change their names or acquire or divest subsidiaries and affiliates.

[36]In November 2019, DOJ charged U.S.-based company Aventura Technologies, Inc. with, among other things, conspiracy to commit wire fraud and mail fraud by selling security and surveillance equipment from PRC-based manufacturers and claiming such equipment was manufactured instead by Aventura Technologies. Complaint, *U.S. v. Cabasso*, No. 19-cr-582 (E.D.N.Y. Nov. 6, 2019). In March 2024, Aventura Technologies pleaded guilty to this charge. Standard Plea Form, *U.S. v. Cabasso*, No. 19-cr-582 (E.D.N.Y. Mar. 19, 2024).

[37]GAO, *Fraud In Federal Programs: FinCEN Should Take Steps to Improve the Ability of Inspectors General to Determine Beneficial Owners of Companies*, GAO-25-107143 (Washington, D.C.: Apr. 8, 2025. Publicly released on Apr. 28, 2025. Reissued with revisions on June 9, 2025).

Agency Comments

We provided a draft of this report to DOD, DOE, DHS, DOJ, State, and Treasury for review and comment. DOE, DHS, DOJ, State, and Treasury did not have any comments on the report. DOD and DHS provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Defense, Energy, Homeland Security, Justice, State, and Treasury; and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Andrew Von Ah at vonaha@gao.gov or Jennifer Franks at franksj@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix I.

//SIGNED//

Andrew Von Ah
Director, Physical Infrastructure

//SIGNED//

Jennifer Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts

Andrew Von Ah, vonaha@gao.gov

Jennifer Franks, franksj@gao.gov

Staff Acknowledgements

In addition to the contacts named above, Saar Dagani (Assistant Director), Roshni Davé (Assistant Director), Jeffrey Knott (Assistant Director), Antoine Clark (Analyst in Charge), Christopher Businsky, Melanie Diemel, Gina Hoover, Charles Hubbard, Joshua Parr, Brandon Sanders, Michael Soressi, Mary Turgeon, Laurel Voloder, and Michelle Weathers made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us