

OMB Action Needed to Ensure Agencies Secure Their Networked Devices

GAO-26-108937

September 2026

A report to congressional committees

Contact: David B. Hinchman at hinchmand@gao.gov

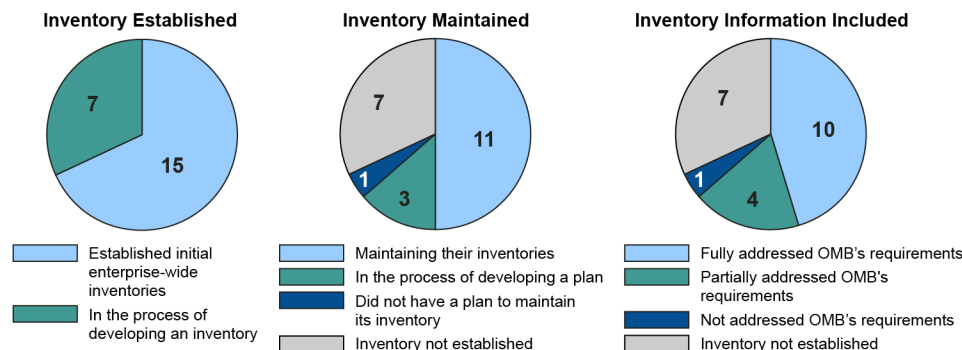
What GAO Found

The nation's infrastructure relies on information systems to support its varied functions. This includes the networked Internet of Things (IoT) and operational technology (OT) devices that interact with the physical world, including in building maintenance systems and specialized equipment in hospitals and laboratories.

Responsible federal agencies have issued guidance, best practices, and requirements to help agencies securely procure such devices. For example, the Office of Management and Budget (OMB) has issued requirements to ensure that agencies establish and maintain inventories of their networked devices and process IoT cybersecurity waivers.

However, most agencies have not fully addressed OMB's networked device requirements, which were established in December 2023 and updated in January 2025. Specifically, agencies' initial inventories were required to be completed by September 2024. However, as of September 2026, of the 22 civilian Chief Financial Officer (CFO) Act agencies in GAO's review, 15 had established an inventory, 11 were maintaining their inventories, and 10 had included all required information (such as asset description and software version) for each device. Overall, only seven agencies had fully addressed all three of OMB's requirements. Further, no agencies had reported an IoT cybersecurity waiver.

Status of 22 Agency Networked Device Inventories, as of September 2026



Source: GAO analysis of Chief Financial Officer (CFO) Act agency documentation. | GAO-26-108937

Agencies cited a variety of reasons for not having completed or maintained inventories with required information, including technical and resource constraints and competing priorities. However, OMB has yet to issue updated guidance to agencies that covers fiscal year 2026, leaving agencies without a clear imperative to prioritize implementation of the requirements and a timeline for doing so. Until OMB issues this guidance, agencies will lack appropriate direction on how and when to complete their device inventories. In the absence of inventories, agencies may lack awareness of the number and type of connected devices in their systems and be at risk of not protecting those systems from cyberattacks. Further, without updated guidance and oversight of agencies' implementation of inventory requirements, agencies may continue to struggle to apply appropriate security controls to vulnerable systems—potentially compromising highly sensitive data and systems.

Why GAO Did This Study

Networked technologies and devices are facing increasing cyber threats from around the globe. For example, in July 2026, cyber threat actors disrupted operations in the water sector by modifying passwords to disconnect networked programmable logic controllers, which are a type of OT. Moreover, emerging technologies such as artificial intelligence can compound risks faced by these technologies and devices. The IoT Cybersecurity Improvement Act of 2020 includes provisions for OMB and civilian CFO Act agencies to identify and protect networked devices.

The act also includes provisions for GAO to report every 2 years on IoT guidance and the waiver process through 2026. This final report in a series of three (1) describes guidance and best practices for procuring secure networked devices; and (2) evaluates agencies' progress in addressing networked device cybersecurity.

GAO identified federal agencies with cybersecurity or acquisition responsibilities and described guidance and best practices developed by those agencies for procuring secure networked devices. GAO compared 22 civilian CFO Act agencies' inventory implementation efforts to OMB's requirements. GAO also interviewed relevant agency officials to obtain their views and verify the information provided.

What GAO Recommends

GAO recommends that OMB issue updated cybersecurity guidance for networked IoT and OT devices and oversee agencies' implementation of the requirements. OMB did not provide comments on this report.