December 2024

INTERNET OF THINGS

Federal Actions Needed to Address Legislative Requirements

GAO Highlights

Highlights of GAO-25-107179, a report to congressional committees

Why GAO Did This Study

Cyber threats to IoT—such as a recent cyberattack on a municipal water system—represent a significant national security challenge. The IoT Cybersecurity Improvement Act of 2020 includes provisions for (1) NIST and OMB to establish guidance for securely procuring IoT, and (2) 23 civilian federal agencies to implement IoT cybersecurity requirements. The act also requires OMB to establish a waiver process for those requirements.

The act includes provisions for GAO to report every 2 years on IoT guidance and the waiver process through 2026. This report, the second of three, (1) describes guidance for securely procuring IoT, and (2) evaluates agencies' progress in addressing IoT cybersecurity and waiver requirements.

GAO identified federal agencies with cybersecurity or acquisition responsibilities. GAO then described relevant guidance developed by those agencies covering IoT. It also compared agencies' implementation efforts to the act and OMB's requirements for IoT inventories and waiver processes. GAO also interviewed relevant agency officials.

What GAO Recommends

GAO is making one recommendation to OMB and 10 to nine civilian agencies covered by the IoT Cybersecurity Improvement Act of 2020 to address legislative requirements related to IoT. Eight agencies concurred with our recommendations. The remaining agencies neither agreed nor disagreed with our recommendations.

View GAO-25-107179. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

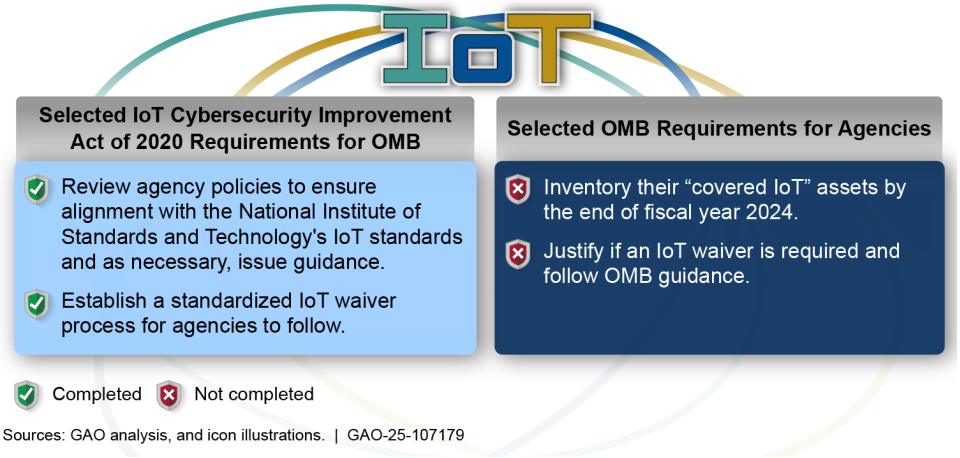
What GAO Found

The Internet of Things (IoT) generally refers to the technology and devices that allow for the connection and interaction of "things" throughout such places as buildings, vehicles, and the transportation infrastructure. The National Institute of Standards and Technology (NIST) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency have issued guidance for securely procuring IoT. For example, NIST has issued cybersecurity guidance for agencies to use in mitigating risk with the acquisition, procurement, and use of IoT at all stages of a system's life cycle. In 2022 and 2023, the Office of Management and Budget (OMB) also issued guidance for ensuring that 23 civilian agencies covered by the IoT Cybersecurity Improvement Act of 2020 address NIST's guidelines, establish IoT inventories, and process IoT cybersecurity waivers.

Many of the 23 civilian agencies have not yet fully addressed OMB's IoT requirements on inventories and waivers. Of these 23 agencies:

- Three stated that they would not complete their inventories by the OMB-established deadline of September 30, 2024, and stated that they plan to do so in fiscal year 2025; six did not provide time frames; and one stated that it does not intend to establish an inventory because it does not have any IoT.
- Six agencies reported granting IoT cybersecurity waivers of certain requirements. However, in following up with these six, officials from five of the agencies stated that they should not have reported waivers. Four of the five subsequently corrected their reported efforts. Additionally, one agency corrected its waiver by removing it, and one (the Department of Health and Human Services) has not yet corrected its waiver. In addition, OMB did not verify any of the reported waiver data and reported erroneous information.

Office of Management and Budget (OMB) and Agency Implementation of Selected Internet of Things (IoT) Requirements



Sources: GAO analysis, and icon illustrations. | GAO-25-107179

Until OMB and agencies ensure that agencies are meeting OMB's requirements, the agencies will not be effectively positioned to assess risks so that they can impose appropriate security requirements and take other mitigating actions.