GAO
Highlights

Highlights of GAO-23-105327, a report to congressional committees

December 2022

CRITICAL INFRASTRUCTURE

Actions Needed to Better Secure Internet-Connected Devices

Why GAO Did This Study

Cyber threats to critical infrastructure IoT and OT represent a significant national security challenge. Recent incidents—such as the ransomware attacks targeting health care and essential services during the COVID-19 pandemic—illustrate the cyber threats facing the nation's critical infrastructure. Congress included provisions in the IoT Cybersecurity Improvement Act of 2020 for GAO to report on IoT and OT cybersecurity efforts.

This report (1) describes overall federal IoT and OT cybersecurity initiatives; (2) assesses actions of selected federal agencies with a lead sector responsibility for enhancing IoT and OT cybersecurity; and (3) identifies leading guidance for addressing IoT cybersecurity and determines the status of OMB's process for waiving cybersecurity requirements for IoT devices. To describe overall initiatives, GAO analyzed pertinent guidance and related documentation from several federal agencies.

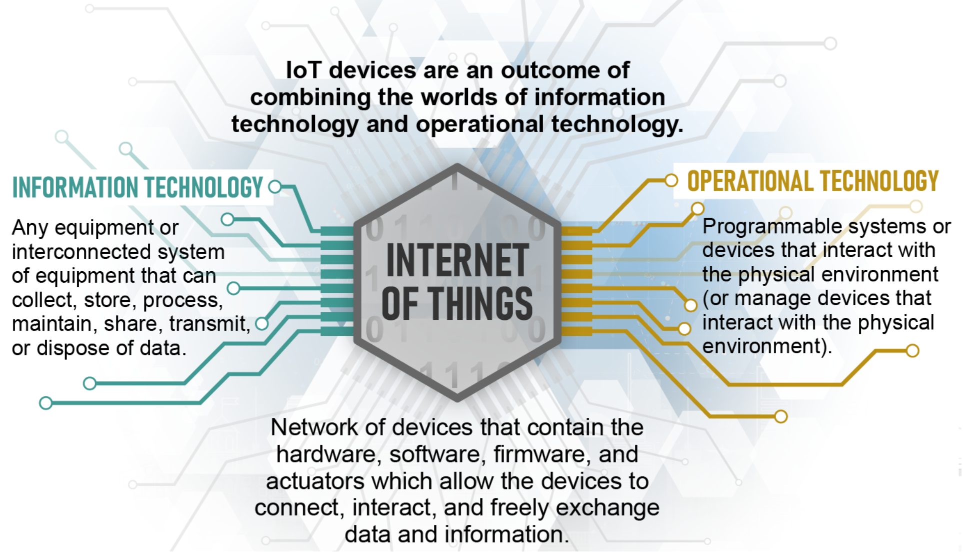
To assess lead agency actions, GAO first identified the six critical infrastructure sectors considered to have the greatest risk of cyber compromise. From these six, GAO then selected for review three sectors that had extensive use of IoT and OT devices and systems. The three sectors were energy, healthcare and public health, and transportation systems. For each of these, GAO analyzed documentation, interviewed sector officials, and compared lead agency actions to federal requirements.

View GAO-23-105327. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

What GAO Found

The nation's critical infrastructure sectors rely on electronic systems, including Internet of Things (IoT) and operational technology (OT) devices and systems. IoT generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of "things," throughout such places as buildings, transportation infrastructure, or homes. OT are programmable systems or devices that interact with the physical environment, such as building automation systems that control machines to regulate and monitor temperature.

Figure: Overview of Connected IT, Internet of Things (IoT), and Operational Technology


IoT devices are an outcome of combining the worlds of information technology and operational technology.
INFORMATION TECHNOLOGY
Any equipment or interconnected system of equipment that can collect, store, process, maintain, share, transmit, or dispose of data.
INTERNET OF THINGS
OPERATIONAL TECHNOLOGY
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).
Network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

Source: GAO; images: ZinetroN/stock.adobe.com, Stockgiu/stock.adobe.com, yershovoleksandr/stock.adobe.com. | GAO-23-105327

To help federal agencies and private entities manage the cybersecurity risks associated with IoT and OT, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) have issued guidance and provided resources. Specifically, CISA has published guidance, initiated programs, issued alerts and advisories on vulnerabilities affecting IoT and OT devices, and established working groups on OT. NIST has published several guidance documents on IoT and OT, maintained a center of cybersecurity excellence, and established numerous working groups. In addition, the Federal Acquisition Regulatory Council is considering updates to the Federal Acquisition Regulation to better manage IoT and OT cybersecurity risks.

Selected federal agencies with a lead role have reported various cybersecurity initiatives to help protect three critical infrastructure sectors with extensive use of IoT or OT devices and systems.

GAO also analyzed documentation, interviewed officials from the selected sectors, and compared those sector's cybersecurity efforts to federal requirements. GAO also interviewed OMB officials on the status of the mandated waiver process.

What GAO Recommends

GAO is making eight recommendations to the lead agencies of the reviewed sectors—the Departments of Energy, Health and Human Services, Homeland Security, and Transportation. GAO is recommending that each department (1) establish and use metrics to assess the effectiveness of sector IoT and OT cybersecurity efforts and (2) evaluate sector IoT and OT cybersecurity risks. GAO is also making one recommendation to OMB to expeditiously establish the required IoT cybersecurity waiver process.

The Departments of Homeland Security and Transportation concurred with the recommendations while Energy said it would not respond to the recommendations until after further coordination with other agencies. Health and Human Services neither agreed nor disagreed with the recommendations but noted planned actions. Specifically, the department said it planned to update its sector-specific plan but asserted that it cannot compel adoption of the plan in the private sector. GAO recognizes the voluntary character of the relationship between the department and the critical infrastructure sector. However, establishing IoT and OT specific metrics will provide a basis for the department to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision-making.

OMB stated that the agency is targeting November 2022 for release of guidance on the waiver process. As of November 22, 2022, OMB had not yet issued this guidance.

Title: Sector Lead Agencies' Internet of Things (IoT) or Operational Technology (OT) Cybersecurity Initiatives

Sector (Lead Federal Agency)	Examples of IoT or OT Initiatives
Energy (Department of Energy)	**Considerations for OT Cybersecurity Monitoring Technologies** guidance provides suggested evaluation considerations for technologies to monitor OT cybersecurity of systems that, for example, distribute electricity through the grid. **Cybersecurity for the Operational Technology Environment** methodology aims to enhance energy sector threat detection of anomalous behavior in OT networks, such as electricity distribution networks.
Healthcare and public health (Department of Health and Human Services)	**Pre-market Guidance for Management of Cybersecurity** identifies issues related to cybersecurity for manufacturers to consider in the design and development of their medical devices, such as diagnostic equipment. **Post-market Management of Cybersecurity in Medical Devices** provides recommendations for managing cybersecurity vulnerabilities for marketed and distributed medical devices, such as infusion pumps.
Transportation systems (Departments of Homeland Security and Transportation)	**Surface Transportation Cybersecurity Toolkit** is designed to provide informative cyber risk management tools and resources for control systems that, for example, function on the mechanics of the vessel. **Department of Homeland Security's Transportation Security Administration's Enhancing Rail Cybersecurity Directive** requires actions, such as conducting a cybersecurity vulnerability assessment and developing of cybersecurity incident response plans for higher risk railroads.

Source: GAO analysis of agency documentation | GAO-23-105327

However, none of the selected lead agencies had developed metrics to assess the effectiveness of their efforts. Further, the agencies had not conducted IoT and OT cybersecurity risk assessments. Both of these activities are best practices. Lead agency officials noted difficulty assessing program effectiveness when relying on voluntary information from sector entities. Nevertheless, without attempts to measure effectiveness and assess risks of IoT and OT, the success of initiatives intended to mitigate risks is unknown.

The Internet of Things Cybersecurity Improvement Act of 2020 generally prohibits agencies from procuring or using an IoT device after December 4, 2022, if that device is considered non-compliant with NIST-developed standards. Pursuant to the act, in June 2021 NIST issued a draft guidance document that, among other things, provides information for agencies, companies and industry to receive reported vulnerabilities and for organizations to report found vulnerabilities. The act also requires the Office of Management and Budget (OMB) to establish a standardized process for federal agencies to waive the prohibition on procuring or using non-compliant IoT devices if waiver criteria detailed in the act are met.

As of November 22, 2022, OMB had not yet developed the mandated process for waiving the prohibition on procuring or using non-compliant IoT devices. OMB officials noted that the waiver process requires coordination and data gathering with other entities. According to OMB, it is targeting November 2022 for the release of guidance on the waiver process. Given the act's restrictions on agency use of non-compliant IoT devices beginning in December 2022, the lack of a uniform waiver process could result in a range of inconsistent actions across agencies.