GAO@100 Highlights

Highlights of GAO-21-105325, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

July 28, 2021

CYBERSECURITY AND INFORMATION TECHNOLOGY

Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas

Why GAO Did This Study

The nation's critical infrastructures and federal agencies are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. Each year, the federal government spends more than $100 billion on cybersecurity and IT investments.

GAO has long stressed the continuing and urgent need for effective cybersecurity, as underscored by recent events that have illustrated persistent and evermore sophisticated cyber threats and incidents. Moreover, many IT investments have failed, performed poorly, or suffered from ineffective management. Accordingly, GAO has included information security on its high-risk list since 1997 and added improving the management of IT acquisitions and operations in 2015. In its March 2021 high-risk series update, GAO reported that significant attention was needed in both of these important areas.

GAO was asked to testify on federal agencies' efforts to address cybersecurity and the management of IT. For this testimony, GAO relied on selected products it previously issued.

What GAO Recommends

Federal agencies have implemented about 73 percent of the approximately 5,100 recommendations that GAO has made since 2010 on cybersecurity and IT management. However, about 950 cybersecurity and approximately 300 IT recommendations have not been implemented. Actions are needed on these to successfully address the high-risk areas.

View GAO-21-105325. For more information, contact Carol C Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

In March 2021, GAO issued its high-risk series update and emphasized that federal agencies' needed to implement numerous critical actions to strengthen the nation's cybersecurity and information technology (IT) management efforts. In the update, GAO reiterated the importance of agencies addressing four major cybersecurity challenges facing the nation: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. Overall, the federal government has to move with a greater sense of urgency to fully address key cybersecurity challenges. In particular:

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace**. In September 2020, GAO reported that the White House's national cyber strategy and associated implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed.
- **Mitigate global supply chain risks**. GAO reported in December 2020 that few of the 23 civilian federal agencies it reviewed implemented foundational practices for managing information and communication technology supply chain risks.
- **Address weaknesses in federal agencies information security programs.** GAO reported in July 2019 that 23 agencies almost always designated a risk executive, but had not fully incorporated other key risk management practices, such as establishing a process for assessing agency-wide cybersecurity risks.

In its March update, GAO also stressed the importance of the Office of Management and Budget (OMB) and federal agencies fully implementing critical actions recommended to improve the management of IT to better manage tens of billions of dollars in IT investments. GAO emphasized, for example, that

- OMB had demonstrated its leadership commitment to improving IT management, but sustaining this commitment was critically important;
- twenty-one of 24 federal agencies had not yet implemented recommendations to fully address the role of Chief Information Officers, including enhancing their authorities;
- OMB and agencies needed to address modernization challenges and workforce planning weaknesses; and
- agencies could take further action to reduce duplicative IT contracts and reduce the risk of wasteful spending.

Until OMB and federal agencies take critical actions to strengthen efforts to address these important high-risk areas, longstanding and pervasive weaknesses will likely continue to jeopardize the nation's cybersecurity and management of IT.