GAO@100 Highlights

Highlights of GAO-21-422T, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

April 2021

INFORMATION TECHNOLOGY AND CYBERSECURITY

Significant Attention Is Needed to Address High-Risk Areas

Why GAO Did This Study

The effective management and protection of IT has been a longstanding challenge in the federal government. Each year, the federal government spends more than $100 billion on IT and cyber-related investments; however, many of these investments have failed or performed poorly and often have suffered from ineffective management.

Accordingly, GAO added improving the management of IT acquisitions and operations as a high-risk area in February 2015. Information security has been on the high-risk area since 1997. In its March 2021 high-risk update, GAO reported that significant actions were required to address IT acquisitions and operations. Further, GAO noted the urgent need for agencies to take 10 specific actions on four major cybersecurity challenges.

GAO was asked to testify on federal agencies' efforts to address the management of IT and cybersecurity. For this testimony, GAO relied primarily on its March 2021 high-risk update and selected prior work across IT and cybersecurity topics.

What GAO Recommends

Federal agencies have fully implemented about 75 percent of the approximately 4,700 recommendations that GAO has made since 2010; however, many critical recommendations have not been implemented—over 400 on IT management and more than 750 on cybersecurity.

View GAO-21-422T. For more information, contact Kevin Walsh at (202) 512-6151 or WalshK@gao.gov.

What GAO Found

In its March 2021 high-risk series update, GAO reported that significant attention was needed to improve the federal government's management of information technology (IT) acquisitions and operations, and ensure the nation's cybersecurity. Regarding management of IT, overall progress in addressing this area has remained unchanged. Since 2019, GAO has emphasized that the Office of Management and Budget (OMB) and covered federal agencies need to continue to fully implement critical requirements of federal IT acquisition reform legislation, known as the Federal Information Technology Acquisition Reform Act (FITARA), to better manage tens of billions of dollars in IT investments. For example:

- OMB continued to demonstrate leadership commitment by issuing guidance to implement FITARA statutory provisions, but sustained leadership and expanded capacity were needed to improve agencies' management of IT.
- Agencies continued to make progress with reporting FITARA milestones and plans to modernize or replace obsolete IT investments, but significant work remained to complete these efforts.
- Agencies improved the involvement of their agency Chief Information Officers in the acquisition process, but greater cost savings could be achieved if IT acquisition shortcomings, such as reducing duplicative IT contracts, were addressed.

In March 2021, GAO reiterated the need for agencies to address 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. GAO identified 10 actions for agencies to take to address these challenges. However, since 2019, progress in this area has regressed—GAO's 2021 rating of leadership commitment declined from met to partially met. To help address the leadership vacuum, in January 2021, Congress enacted a statute establishing the Office of the National Cyber Director. Although the director position has not yet been filled, on April 12 the President announced his intended nominee. Overall, the federal government needs to move with a greater sense of urgency to fully address 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 cyber strategy and 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**. In December 2020, GAO reported that few of the 23 civilian federal agencies it reviewed implemented foundational practices for managing information and communication technology supply chain risks.
- **Enhance the federal response to cyber incidents**. In July 2019, GAO reported that most of 16 selected federal agencies had deficiencies in at least one of the activities associated with incident response processes.