United States Government Accountability Office

Testimony

Before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

For Release on Delivery
Expected at 9:00 a.m. ET
Friday, April 16, 2021

INFORMATION TECHNOLOGY AND CYBERSECURITY

Significant Attention Is Needed to Address High-Risk Areas

Statement of Kevin Walsh, Director,
Information Technology and Cybersecurity

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-422T

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.

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee:

I am pleased to be here today to discuss improving the federal government's management of information technology (IT) and enhancing our nation's cybersecurity. As you know, the effective and efficient management 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. Yet, we have long reported that many of these investments have failed or performed poorly and often have suffered from ineffective management. Consequently, we added improving the management of IT acquisitions and operations to our high-risk areas for the federal government in February 2015.[1] In March 2021, we reported that while progress had been made in addressing the high-risk area of IT acquisitions and operations, significant actions were required by federal agencies to build on this progress.[2]

With regard to cybersecurity, federal agencies and our nation's critical infrastructures are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. However, the increasingly sophisticated threats and frequent cyber incidents underscore the continuing and urgent need for effective information security.

We have designated information security as a government-wide high-risk area since 1997.[3] In 2003, we added the protection of critical infrastructure to the information security high-risk area, and, in 2015, we further expanded this area to include protecting the privacy of personally

[1]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015). GAO's high-risk program identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation to address economy, efficiency, or effectiveness challenges. Every 2 years, we issue an update that describes the status of these high-risk areas and actions that are still needed to assure further progress, and identifies new high-risk areas needing attention by Congress and the executive branch.

[2]GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[3]GAO, *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: Feb. 1997).

identifiable information.[4] In September 2018, and again in March 2021, we emphasized the critical need for the federal government to take 10 specific actions[5] to address four major cybersecurity challenges that the federal government and other entities face: (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.[6]

My remarks today will discuss federal agencies' efforts to address our high-risk areas focused on the management of IT and cybersecurity. The information in this statement is based primarily on our March 2021 high-risk update, which relied on reports we had issued as of mid-January 2021. This statement also includes selected updates based on information we obtained and analyzed from officials at various federal agencies regarding efforts to address recommendations we have previously made. More detailed information about our scope and methodology can be found in our reports and testimonies cited throughout this statement.

We conducted the work on which this statement is based in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

Background

Congress has long recognized that federal agencies accomplish their missions more quickly, effectively, and economically through the use of IT systems. These systems provide essential services that are critical to the health, economy, and defense of the nation. Toward this end, the federal government has projected that it will spend approximately $104 billion on IT investments in fiscal year 2021.

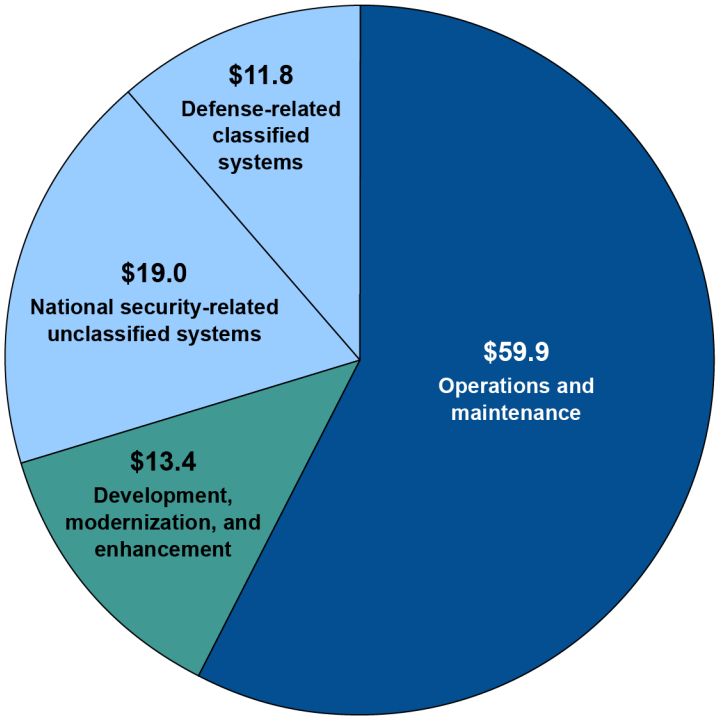
[4]GAO, *High-Risk Series: An Overview*, HR-97-1 (Washington, D.C.: Feb. 1997); *High-Risk Series: An Update,* GAO-03-119 (Washington, D.C.: Jan. 2003); and GAO-15-290.

[5]The 10 actions are identified in figure 3 of this statement.

[6]See GAO, *High-Risk Series*: *Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021) and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

A large majority of these investments are intended to support the operation and maintenance of existing IT systems—such as those that support tax filings, Census survey information, and veterans' health records. Additionally, these investments are to support system development, modernization, and enhancement activities including software upgrades, the replacement of legacy IT, and new technologies. The planned fiscal year 2021 spending also includes costs for defense-related classified systems and national security-related unclassified systems, which support cyber activities.[7] Figure 1 reflects the planned fiscal year 2021 spending for IT investments.

Figure 1: Summary of Planned Fiscal Year 2021 Spending on Information Technology (IT) Investments, as of January 2021 (Dollars in billions)



Source: GAO analysis of Office of Management and Budget IT Dashboard reported data. | GAO-21-422T

[7]The detailed information for defense-related classified systems and national security-related unclassified systems is not publicly distributed; these totals were included in the Department of Defense IT budget documentation for fiscal year 2021.

Notwithstanding the billions of dollars spent annually, federal IT investments often suffer from a lack of disciplined and effective management in areas such as project planning, requirements definition, and program oversight and governance. These investments too frequently fail to deliver capabilities in a timely manner, incur cost overruns, and/or experience schedule slippages while contributing little to mission-related outcomes. For example, our work has highlighted the following shortcomings in the federal government's management of IT investments:

- The Internal Revenue Service has encountered long-standing IT operational challenges. As of October 2020, these challenges included computers freezing or taking excessive time to reboot and a lack of timeliness to address improvements. The Internal Revenue Service's IT systems support the collection of more than $3 trillion in taxes and the distribution of more than $400 billion in refunds annually.[8]
- The United States Coast Guard decided to terminate its Integrated Health Information System project in 2015. As reported by the agency in August 2017, approximately $60 million had been spent over 7 years on this project, which resulted in no equipment or software that could be used for future efforts.[9]
- The Department of Veterans Affairs' Financial and Logistics Integrated Technology Enterprise program was intended to be delivered by 2014 at a total estimated cost of $609 million, but was terminated in October 2011 due to challenges in managing the program.[10]
- The Department of Defense canceled its Expeditionary Combat Support System in December 2012 after spending more than a billion

[8]GAO, *Information Technology: IRS Needs to Address Operational Challenges and Opportunities to Improve Management*, GAO-21-178T (Washington, D.C.: Oct. 7, 2020).

[9]GAO, *Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process*, GAO-18-59 (Washington, D.C.: Jan. 24, 2018).

[10]GAO, *Information Technology: Actions Needed to Fully Establish Program Management Capability for VA's Financial and Logistics Initiative,* GAO-10-40 (Washington, D.C.: Oct. 26, 2009).

dollars and not deploying the system within 5 years of initially obligating funds.[11]

- The Department of Homeland Security ended its Secure Border Initiative Network program in January 2011, after the department obligated more than $1 billion for the program.[12]

In addition to failures in managing IT investments, security risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing. Compounding this risk, systems and networks used by federal agencies and our nation's critical infrastructure often are interconnected with other internal and external systems and networks, including the internet. With this greater connectivity, threat actors are increasingly willing and capable of conducting a cyberattack on our nation's critical infrastructure that could be disruptive and destructive.

Recent events highlight the significant cyber threats facing the nation and the range of consequences that these attacks pose.

- In December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive and alert explaining that an advanced persistent threat actor had compromised the supply chain of a network management software suite and inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product.[13] The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.

[11]GAO, *DOD Financial Management: Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals*, GAO-12-134 (Washington, D.C.: Feb. 28, 2012) and *DOD Business Transformation: Improved Management Oversight of Business System Modernization Efforts Needed*, GAO-11-53 (Washington, D.C.: Oct. 7, 2010).

[12]See, for example, GAO, *Secure Border Initiative: DHS Needs to Strengthen Management and Oversight of Its Prime Contractor*, GAO-11-6 (Washington, D.C.: Oct.18, 2010); *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340 (Washington, D.C.: May 5, 2010); and *Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk*, GAO-10-158 (Washington, D.C.: Jan. 29, 2010).

[13]CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020) and *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, Alert AA20-352A (Dec. 17, 2020).

- In February 2021, CISA issued an alert explaining that cyber threat actors had obtained unauthorized access to a U.S. water treatment facility's industrial controls systems and attempted to increase the amount of a caustic chemical that is used as part of the water treatment process.[14] According to CISA, threat actors likely accessed systems by exploiting cybersecurity weakness, including poor password security and an outdated operating system.
- In March 2021, CISA issued an emergency directive and alert explaining that CISA's partners had observed active exploitation of vulnerabilities in Microsoft Exchange Server—a product for email inboxes, calendars, and collaboration tools.[15]

Overview of Federal Information Technology Acquisition Reform Legislation

As part of its effort to reform the government-wide management of IT, Congress and the President enacted the Federal Information Technology Acquisition Reform Act, commonly referred to as FITARA, in December 2014.[16] This legislation was intended to improve covered agencies' acquisitions of IT and enable Congress to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings.[17] The law includes specific requirements related to seven areas:

- **Agency Chief Information Officers (CIO) authority enhancements.** CIOs have the authority to, among other things, approve IT-related budget requests and contracts of their respective agencies. Additionally, CIOs are required to certify that IT investments are adequately implementing incremental development.

[14]CISA, *Compromise of U.S. Water Treatment Facility*, Alert AA21-042A (Feb. 11, 2021).

[15]CISA, *Mitigate Microsoft Exchange Server Vulnerabilities*, Alert AA21-062A (Mar. 3, 2021) and *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021).

[16]Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

[17]The provisions apply to the agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b). These agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. However, FITARA has generally limited application to the Department of Defense.

- **Federal data center consolidation initiative.** Provide a strategy for consolidating and optimizing their data centers and issue quarterly updates on the progress made, among other things.
- **Enhanced transparency and improved risk management.** Make detailed information on federal IT investments publicly available, and require CIOs to categorize their investments by level of risk. Moreover, for certain investments consistently categorized with a high level of risk, the CIO and investment's program manager are required to conduct a review aimed at identifying and addressing the causes of the risk.
- **Portfolio review.** Review IT investment portfolios annually in order to, among other things, increase efficiency and effectiveness and identify potential waste and duplication. Additionally, the Office of Management and Budget (OMB) is required to quarterly report associated cost savings to Congress.
- **Expansion of training and use of IT acquisition cadres.** Update acquisition human capital plans to support timely and effective IT acquisitions. In doing so, the law calls for agencies to consider, among other things, establishing IT acquisition cadres or developing agreements with other agencies that have such cadres.
- **Government-wide software purchasing program.** Allow for the purchase of a government-wide software licensing agreement that is available for use by agencies. Specifically, the General Services Administration is to develop a strategic sourcing initiative to enhance government-wide acquisition and management of software.
- **Maximizing the benefit of the Federal Strategic Sourcing Initiative.** Compare federal purchases of services and supplies to what is offered under the Federal Strategic Sourcing Initiative.

Recognizing the importance of agencies' continued implementation of FITARA provisions, Congress and the President enacted the FITARA Enhancement Act of 2017 to extend selected provisions beyond their original dates of expiration.[18] Specifically, the expiration dates for the enhanced transparency, improved risk management, and portfolio review provisions, which were set to expire in 2019, were removed. The act also extended the expiration date for the federal data center consolidation initiative from 2018 to 2020.

[18]FITARA Enhancement Act of 2017, Pub. L. No. 115-88, 131 Stat. 1278 (2017).

In addition to FITARA, Congress and the President enacted a law in 2017 to authorize the availability of funding mechanisms to help further agencies' efforts to modernize IT. Specifically, the Modernizing Government Technology (MGT) Act, as it is commonly known, authorized agencies to establish working capital funds for use in transitioning away from legacy IT systems, as well as for addressing evolving threats to information security.[19] The law also created the Technology Modernization Fund within the Department of the Treasury, from which agencies can "borrow" money to retire and replace legacy systems, as well as to acquire or develop systems.

To better assist federal agencies in implementing reform laws and adhere to FITARA requirements, the OMB issued related guidance.[20] Specifically, OMB issued guidance related to the implementation of FITARA and the MGT Act that provided agencies additional information regarding, among other things, the role of the CIO and the administration of IT working capital funds. In August 2020, we reported that agencies had made progress in implementing key reform legislation and OMB guidance, but work remained to fully address the gaps we previously identified.[21]

Effective Practices for Implementing FITARA Requirements

In April 2019, we reported on 12 practices that have helped agencies effectively implement one or more of the FITARA provisions.[22] These practices included overarching approaches as well as specific actions that, when implemented, can enable agencies to realize IT management improvements, such as decommissioning old systems and achieving cost savings. Figure 2 identifies these overarching practices as well as specific actions related to FITARA requirements.

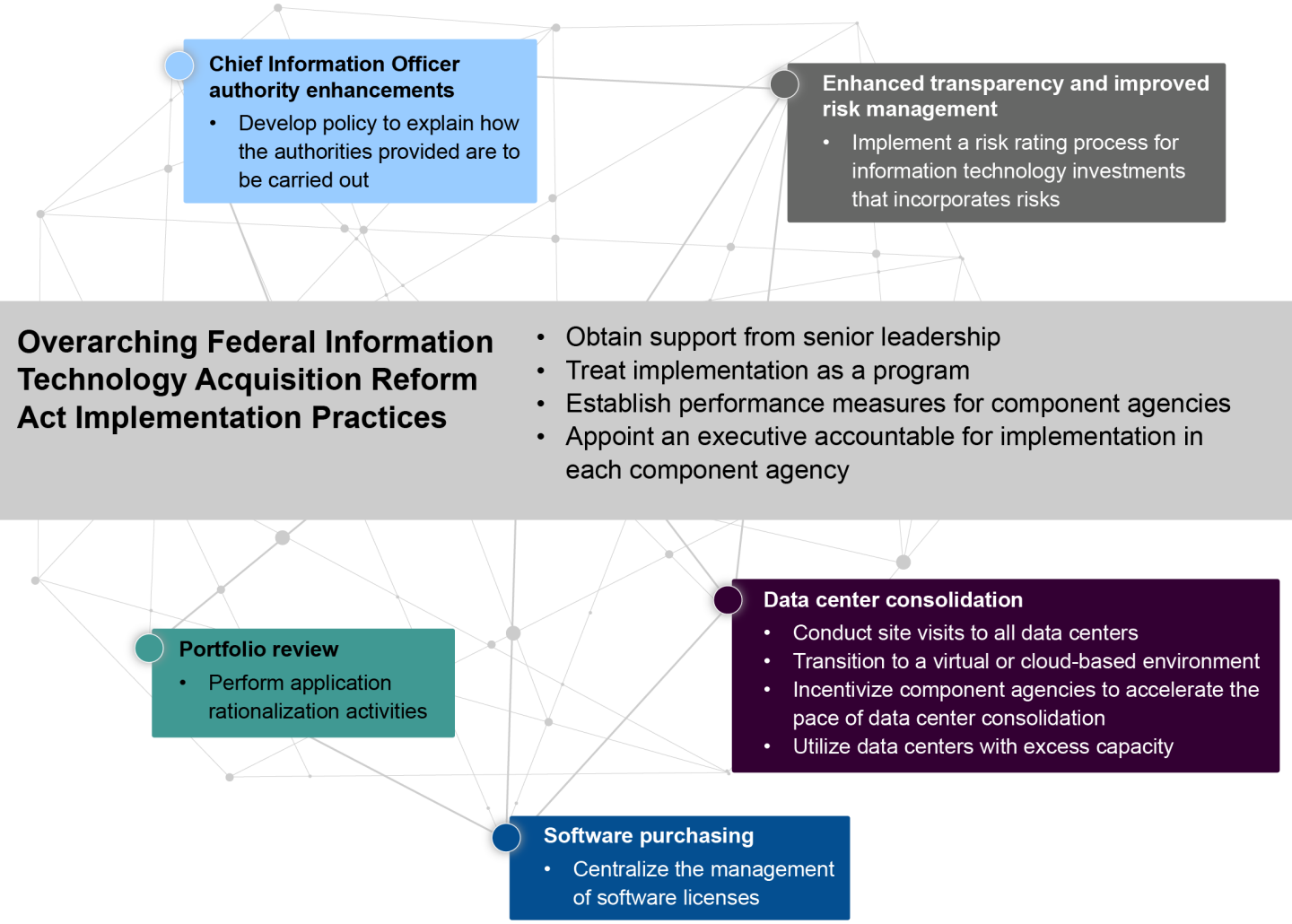
[19]National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586 (2017).

[20]OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015); *Data Center Optimization Initiative (DCOI),* Memorandum M-16-19 (Washington, D.C.: Aug. 1, 2016); *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018); *Funding Guidelines for Agencies Receiving Disbursements from the Technology Modernization Fund* (Washington, D.C.: Mar. 12, 2018); and *Update to Data Center Optimization Initiative (DCOI)*, Memorandum M-19-19 (Washington, D.C.: June 25, 2019).

[21]GAO, *Information Technology: Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity,* GAO-20-691T (Washington, D.C.: Aug. 3, 2020).

[22]GAO, *Information Technology: Effective Practices Have Improved Agencies' FITARA Implementation*, GAO-19-131 (Washington, D.C.: Apr. 29, 2019).

Figure 2: Practices That Selected Agencies Used to Effectively Implement Key Provisions of the Federal Information Technology Acquisition Reform Act (FITARA)



Source: GAO analysis of Office of Management and Budget IT Dashboard reported data. | GAO-21-422T

Reform Legislation and Congressional Oversight Continue to Be Important for Federal Agencies' Progress in Managing IT and Cybersecurity

Reform legislation and congressional oversight are important to agencies' progress in better managing the large investment the federal government continues to make in IT. In February 2015, we reported that the federal government's continued experience with failed and troubled IT projects was compounded by inconsistent implementation of numerous initiatives

undertaken by the executive branch to better manage IT investments.[23] As a result, we stressed that the government would likely continue to produce disappointing results and miss opportunities to improve IT management, reduce costs, and improve services to the public, unless needed actions were taken.

We also reported that it would be more difficult for stakeholders, including Congress and the public, to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings. We emphasized that FITARA should be expeditiously implemented and that, to help ensure desired improvements were achieved, congressional oversight of agencies' implementation efforts was essential.

In November 2015, this committee began monitoring agencies' progress by issuing biannual scorecards that tracked and graded agency efforts to address FITARA requirements, among other things.[24] Specifically, the scorecards focused on FITARA provisions related to four areas: CIO authority, data center consolidation, transparency of risks, and IT investment portfolio review.

In 2016 and 2017, Congress and the President enacted additional legislation aimed at improving the management of software licensing[25] and establishing IT-specific working capital funds.[26] Accordingly, following those years, this committee incorporated monitoring agencies' progress in managing software and setting up working capital funds into the scorecard.

In June 2019, the scorecard was further updated to reflect a grade for cybersecurity and, most recently, in December 2020, agencies' progress

[23]GAO-15-290.

[24]The scorecard grades are based primarily on publicly available data reported by OMB and covered federal agencies.

[25]The Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, or the "MEGABYTE Act" further enhances CIOs' management of software licenses by requiring agency CIOs to establish an agency software licensing policy and a comprehensive software license inventory to track and maintain licenses, among other requirements. Pub. L. No. 114-210, 130 Stat. 824 (2016). Also, see GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide,* GAO-14-413 (Washington, D.C.: May 22, 2014).

[26]National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586 (2017).

toward transitioning off of expiring telecommunications contracts[27] was added. In addition, federal agencies are graded on the progress made toward institutionalizing their respective CIOs' ability to report directly to the head or deputy of the agency.

Significant Attention Is Needed to Address IT Management and Cybersecurity High-Risk Areas

In the March 2021 update to our high-risk series, we reported that significant attention was needed to address challenges related to improving the federal government's management of IT acquisitions and operations, as well as ensuring the cybersecurity of the nation.[28] Regarding management of IT, overall progress in addressing this area has remained unchanged. Since 2019, we have emphasized that OMB and other federal agencies need to continue to fully implement critical FITARA requirements. However, since 2019, progress in the area of cybersecurity has regressed—our 2021 rating of leadership commitment declined from met to partially met.[29]

Congressional action has aided progress in (1) building the federal government's capacity (i.e., people and resources) for better managing IT acquisitions and operations and (2) establishing an office responsible for, among other things, improving the coordination of cybersecurity policy and operations across the executive branch.[30] However, further agency actions can be taken to improve IT acquisitions and operations and strengthen federal cybersecurity.

Agencies Need to Take Critical Actions to Improve the Management of IT Acquisitions and Operations

As part of our March 2021 high-risk update, we reported that OMB and other federal agencies should continue to fully implement critical requirements of federal IT acquisition reform legislation to better manage tens of billions of dollars in IT investments.[31] In particular, sustained leadership commitment, progress in reporting modernization plans, and

[27]Delays in the previous telecommunication contract transition resulted in hundreds of millions of dollars in missed savings. Also see GAO, *Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays,* GAO-20-155 (Washington, D.C.: Apr. 7, 2020).

[28]GAO-21-119SP.

[29]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[30]Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021), established, within the Executive Office of the President, the Office of the National Cyber Director.

[31]GAO-21-119SP and GAO-21-288.

improved involvement of the CIO in the acquisition process remain key areas of focus.

Sustained Leadership and Expanded Capacity Can Improve Agencies' Management of IT

As noted in our 2021 update, OMB continued to demonstrate its leadership commitment by issuing guidance to implement FITARA statutory provisions. However, maintaining this current level of leadership with the new administration is important for ensuring that agencies succeed. As reflected in the major federal agencies' progressing scorecard grades issued by this committee, congressional focus has led to improvement in managing IT acquisitions. Notwithstanding OMB's leadership commitment, sustained executive branch and congressional attention will continue to be essential to ensure progress in addressing long-standing IT management challenges.

Beyond leadership, our update to the IT acquisition and operations high-risk area also stressed that federal agencies' capacity to better manage and modernize IT has been limited. As previously mentioned, in December 2017, the Technology Modernization Fund was established by the MGT Act to assist agencies with funding to replace aging IT systems.[32] In December 2019, we reported that Congress had appropriated $125 million to the fund but that challenges with covering the cost of operating the fund had resulted in fewer funds being available than anticipated for the new projects.[33] As of April 2021, approximately $89 million had been awarded to 11 projects across seven federal agencies.

On March 11, 2021, Congress and the President enacted legislation that appropriated an additional $1 billion to be available until September 30, 2025 to carry out the purposes of the fund.[34] Our prior work also identified the need for OMB to (1) develop a plan to address the challenges with operating the fund and (2) clarify guidance for agencies' cost estimates associated with the awarded projects. However, as of April 2021, our recommendations had not yet been implemented. Without OMB clarifying the requirement that agencies follow cost estimating processes, agencies

[32]National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115–91, title X, div. A, subtitle G, 131 Stat. 1283, 1586 (2017).

[33]GAO, *Technology Modernization Fund: OMB and GSA Need to Improve Fee Collection and Clarify Cost Estimating Guidance for Awarded Projects,* GAO-20-3 (Washington, D.C.: Dec. 12, 2019).

[34]American Rescue Plan Act of 2021, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 79 (2021).

are at risk of continuing to provide unreliable cost information in their proposals.

We have also previously reported that effective workforce planning is key to addressing the federal government's IT challenges and ensuring that agencies have staff with the necessary knowledge, skills, and abilities to execute a range of management functions that support agencies' missions and goals. In this regard, we have stressed that implementing workforce planning activities can facilitate the success of major IT acquisitions.[35]

In October 2019, our report on major agencies' implementation of IT workforce planning strategies noted that 23 of 24 agencies had at least partially implemented three of eight key workforce planning activities, including identifying staffing needs and assessing gaps.[36] However, most of the agencies had minimally implemented or had not implemented five other workforce planning activities, including developing strategies to address those gaps. The agencies provided various reasons for their limited progress in implementing workforce planning activities, including competing priorities and limited resources.

We made a recommendation to 18 of the 24 agencies to fully implement the eight key IT workforce planning activities. Thirteen agencies agreed with the recommendation, while the other five expressed a range of views. Further, a number of agencies made progress toward implementing the recommendation; however, as of April 2021, none of the agencies had fully implemented the recommendation.

In August 2018, we reported on critical actions needed to address shortcomings and challenges in implementing CIO responsibilities, including the role of the CIO in assessing agency IT workforce needs.[37] Specifically, we reported that the majority of agencies' policies minimally

[35]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[36]GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities,* GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

[37]GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities,* GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

addressed or did not address the role of their CIOs with respect to the IT workforce.

As of March 2021, 21 of the 24 major federal agencies still had not implemented recommendations we made in 2018 regarding modifying their practices to fully address the role of their CIOs, consistent with federal laws and OMB's FITARA guidance. The guidance covers, among other things, enhancing the authority of federal CIOs and ensuring that program staff have the necessary knowledge and skills to effectively acquire IT.

However, we identified the need for OMB to address CIO responsibilities not included in existing guidance—in particular, roles related to IT workforce matters. As we stressed, until OMB updates its guidance to address these responsibilities, CIOs may not have the personnel needed to effectively acquire, maintain, and secure their IT systems. As of April 2021, OMB had not yet taken action to fully address our recommendation.

Agencies Continue to Make Progress in Modernizing or Replacing Obsolete IT Investment

Agencies continue to make progress with reporting FITARA milestones and plans to modernize or replace obsolete IT investments, although work remains to complete these efforts. For example, as we reported in our 2021 high-risk update, four agencies reported the completion of all milestones in their plans to address IT management issues, such as reviewing poorly performing investments and managing agencies' IT portfolios. Eighteen agencies reported milestones that were still in progress or deferred. Two agencies had not reported on their milestone status and other agencies had not updated their status in several years.[38]

Regarding plans to modernize or replace obsolete IT investments, federal agencies are required by OMB to shift their IT services to a cloud computing option when feasible. Toward this end, the agencies we reviewed in 2019 had made progress in implementing cloud services. Specifically, they had established assessment guidance, performed assessments, and implemented these services. Nevertheless, the extent of their progress varied and, as of April 2021, OMB had not yet implemented our recommendation to require agencies to explicitly report

[38]GAO-21-119SP.

the savings and cost avoidance associated with cloud computing investments.[39]

Addressing IT Acquisition Shortcomings Could Achieve Greater Cost Savings

A key component of improving the management of IT is the involvement of the agency CIO in the acquisition process. Toward this end, several agencies had made progress in identifying IT contracts and ensuring that acquisition offices were involved in the process. For example, in 2018 we recommended that 20 agencies improve their CIOs' involvement in the acquisition process. As of April 2021, all but one agency had implemented our recommendation to ensure that acquisition office was involved in the process of identifying IT acquisitions. To their credit, all 20 agencies had issued specific guidance to direct the identification of IT acquisitions. However, as of April 2021, nine agencies had not yet ensured that their CIOs reviewed and approved IT acquisition plans or strategies in accordance with OMB guidance.[40]

Further, as we highlighted in our November 2017 report, CIO involvement in the certification of incremental development also continues to be a focus. For instance, 13 of 17 agencies that lacked adequate incremental development approaches involving their CIOs, fully implemented our 2017 recommendations to improve reporting accuracy and update or establish policies.[41] Nonetheless, our work in 2020 found that selected federal agencies could take further action to reduce duplicative IT contracts and reduce the risk of wasteful spending.[42] Until such actions are implemented, agencies could miss opportunities to identify and realize savings of potentially hundreds of millions of dollars.

[39]GAO, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked,* GAO-19-58 (Washington, D.C.: Apr. 4, 2019).

[40]GAO, *Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions,* GAO-18-42 (Washington, D.C.: Jan. 10, 2018).

[41]GAO, *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017).

[42]GAO, *Information Technology: Selected Federal Agencies Need to Take Additional Actions to Reduce Contract Duplication,* GAO-20-567 (Washington, D.C.: Sept. 30, 2020).

Agencies Need to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges

In March 2021, we reiterated the importance for agencies to take 10 critical actions to address four major cybersecurity challenges facing the nation (see figure 3).[43]

[43]GAO-21-119SP and GAO-21-288.

Figure 3: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government-wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-21-422T

Recent events highlight the urgent need to take these critical actions to address the four major cybersecurity challenges. For example, as previously mentioned, in December 2020, CISA issued an emergency directive and alert regarding an advanced persistent threat actor. Specifically, this threat actor had been observed leveraging, among other techniques, a software supply chain compromise of an enterprise network

management software suite to conduct a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations. According to CISA, this threat poses a grave risk to the federal, state, local, tribal, and territorial governments, as well as critical infrastructure entities and other private sector organizations.

Agencies need to urgently address the 10 critical actions to effectively respond to recent incidents and, thus better position the nation to prevent, or more quickly detect and mitigate the damage of, future cyberattacks. In particular:

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.** The White House's September 2018 National Cyber Strategy and the National Security Council's accompanying June 2019 Implementation Plan detailed the executive branch's approach to managing the nation's cybersecurity. However, in September 2020, we reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed.[44]

  We recommended that the National Security Council work with relevant federal entities to update cybersecurity strategy documents to include goals and resource information, among other things. The National Security Council staff neither agreed nor disagreed with our recommendation and has yet to address it. Moving forward, the new administration needs to either update the existing strategy and plan or develop a new comprehensive strategy that addresses those characteristics.

  We also highlighted the urgent need to clearly define a central role for leading the implementation of the national strategy. Accordingly, we suggested that Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, Congress enacted a statute that established the Office of the National Cyber Director within the Executive Office of the President.[45] The office is to be headed by a National Cyber Director, a presidentially appointed, Senate-confirmed position. Although the director position had not yet

[44]GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).

[45]Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021).

been filled, on April 12, 2021, the President announced his intended nominee. Once this position is filled, the federal government will be better situated to direct activities to overcome the nation's cyber threats and challenges, and to perform effective oversight.

- **Mitigate global supply chain risks.** In December 2020, we reported that few of the 23 civilian agencies we reviewed[46] had implemented foundational practices for managing information and communication technology supply chain risks.[47] In that report, we identified the seven practices from the National Institute of Standards and Technology's guidance that are foundational for an organization-wide approach to information and communication technology supply chain risk management.[48]

  However, we found that none of the 23 agencies had fully implemented all of the supply chain risk management practices and 14 of the 23 agencies had not implemented any of the practices. In a sensitive report issued in October 2020, we made 145 recommendations to the 23 agencies to fully implement foundational practices in their organization-wide approaches to information and communication technology supply chain risk management.[49]

- **Enhance the federal response to cyber incidents**. In July 2019, we reported that most of 16 selected federal agencies had deficiencies in at least one of the activities associated with incident response processes.[50] We and the inspectors general have made thousands of recommendations aimed at improving information security programs and practices—including those relating to incident response

[46]We did not include the Department of Defense because our scope was the civilian agencies.

[47]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

[48]See NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v. 1.1 (Apr. 16, 2018); *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161 (Gaithersburg, Md.: Apr. 2015); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37, Rev. 2 (Gaithersburg, Md.: Dec. 2018); and *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: Mar. 2011).

[49]GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: Oct. 27, 2020).

[50]GAO, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545 (Washington, D.C.: July 26, 2019).

processes over the years; however, many of these recommendations remain unimplemented.

In summary, our March 2021 high-risk update emphasized that significant attention is needed to address challenges related to improving the federal government's management of IT acquisitions and operations, as well as ensuring the cybersecurity of the nation. Specifically, OMB and other federal agencies should continue to fully implement critical requirements of FITARA to better manage the tens of billions of dollars in IT investments. As of December 2020, federal agencies had fully implemented 65 percent of the roughly 1,400 IT management-related recommendations we made since 2010. Agencies should implement our remaining approximately 400 open recommendations related to this high-risk area.

Moreover, although the federal government has made selected improvements, it needs to move with a greater sense of urgency to fully address the four cybersecurity challenges facing the nation. For example, since 2010, agencies have implemented approximately 80 percent of about 3,300 recommendations that we have made related to the challenges. Nevertheless, more than 750 of our recommendations had not been implemented as of December 2020. Until our recommendations are implemented and actions are taken to address the four challenges, the federal government's IT systems, the nation's critical infrastructure, and the personal information of U.S. citizens and others will be increasingly susceptible to the multitude of cyber-related threats that exist.

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Kevin C. Walsh, Director of Information Technology and Cybersecurity, at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Teresa M. Yost (Assistant Director), John Bailey (Analyst-in-Charge), Chris Businsky, Donna Epler, Rebecca Eyler, Gabriel Nelson, and Sukhjoot Singh.