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 2:00 p.m. ET
Monday, August 3, 2020

INFORMATION TECHNOLOGY

Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity

Statement of Carol C. Harris, Director
Information Technology Management Issues

August 3, 2020

GAO Highlights

Highlights of GAO-20-691T, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

INFORMATION TECHNOLOGY

Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity

Why GAO Did This Study

Each year, the federal government invests over $90 billion in IT. Even so, IT investments have too often failed or contributed little to mission-related outcomes. Increasingly sophisticated threats and frequent cyber incidents also underscore the need for effective information security. To focus attention on these concerns, GAO has included both the management of IT acquisitions and operations and cybersecurity on its high-risk list.

For this statement, GAO summarized its key related reports and assessed agencies' progress in implementing the reports' recommendations. Specifically, GAO reviewed the implementation of recommendations on (1) CIO responsibilities, (2) IT acquisition review requirements, (3) data center consolidation, (4) the management of software licenses, and (5) cybersecurity.

What GAO Recommends

Since fiscal year 2010, GAO has made 1,376 recommendations to OMB and agencies to address shortcomings in IT acquisitions and operations, as well as 3,409 recommendations to agencies to improve the security of federal systems. These recommendations addressed, among other things, implementation of CIO responsibilities, oversight of the data center consolidation initiative, management of software licenses, and the efficacy of security programs. Implementing these recommendations is essential to strengthening federal agencies' IT acquisitions, operations, and cybersecurity efforts.

View GAO-20-691T. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

Federal agencies and the Office of Management and Budget (OMB) have taken steps to improve the management of information technology (IT) acquisitions and operations and ensure the nation's cybersecurity through a series of initiatives. As of July 2020, federal agencies had fully implemented 64 percent of the 1,376 IT management-related recommendations that GAO has made to them since fiscal year 2010. Likewise, agencies had implemented 79 percent of the 3,409 security-related recommendations that GAO has made since fiscal year 2010. However, significant actions remain to be completed to build on this progress.

- **Chief Information Officer (CIO) responsibilities**. Laws such as the Federal Information Technology Acquisition Reform Act (FITARA) and related guidance assign 35 key responsibilities to agency CIOs to help address longstanding IT management challenges. In August 2018, GAO reported that none of the 24 selected agencies had established policies that fully addressed the role of their CIO. GAO recommended that OMB and the 24 agencies take actions to improve the effectiveness of CIOs' implementation of their responsibilities. Although most agencies agreed or did not comment, only four of the 27 recommendations have been implemented.
- **CIO IT acquisition review**. According to FITARA, covered agencies' CIOs are required to review and approve IT contracts. Nevertheless, in January 2018, GAO reported that most of the CIOs at 22 covered agencies were not adequately involved in reviewing billions of dollars of IT acquisitions. Since then, agencies implemented 29 out of 39 recommendations made to improve CIO oversight for these acquisitions. Implementing the remaining 10 could increase CIOs' authority and improve the management of IT contracts.
- **Consolidating data centers**. OMB launched an initiative in 2010 to reduce data centers. According to the 24 covered agencies, this initiative has resulted in approximately $4.7 billion in cost savings from fiscal years 2012 through 2019. Even so, additional work remains. As of July 2020, OMB and agencies implemented 133 of the 204 recommendations made to improve the reporting of related cost savings and to achieve optimization targets. Implementing the remaining recommendations could yield additional cost savings.
- **Managing software licenses**. Effective management of software licenses can help avoid purchasing too many licenses that result in unused software. In May 2014, GAO reported that better management of licenses was needed to achieve savings and made 135 recommendations to improve such management. Agencies have implemented 123 of the 135 recommendations. Implementing the remaining 12 could reduce spending and duplication.
- **Ensuring the nation's cybersecurity**. GAO continues to designate information security as a government-wide high-risk area due to increasing cyber-based threats and the persistent nature of security vulnerabilities. Since fiscal year 2010, GAO has made 3,409 recommendations to agencies aimed at addressing cybersecurity challenges. As of July 2020, 79 percent of the recommendations have been implemented. Until the remaining recommendations are addressed, agencies' information and IT systems will be increasingly susceptible to the existing multitude of cyber-related threats.

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

I am pleased to be here today to provide an update on federal agencies' efforts to address our high-risk areas on improving the management of information technology (IT) acquisitions and operations, as well as ensuring the cybersecurity of the nation. The federal government has spent billions of dollars on failed and poorly performing IT investments, which often 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 2019, we reported that, while progress had been made in addressing the high-risk area of IT acquisitions and operations, significant work remained to be completed.[2]

With regard to cybersecurity, the increasingly sophisticated threats and frequent cyber incidents underscore the continuing and urgent need for effective information security. We first identified federal information security as a government-wide high-risk area in 1997.[3] Subsequently, in 2003,[4] we expanded this area to include computerized systems supporting the nation's critical infrastructure, and, in 2015,[5] 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 two 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. Financial benefits to the federal government due to progress in addressing high-risk areas from fiscal years 2006 through 2018 totaled nearly $350 billion.

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

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

[4]See GAO, *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997) and *High-Risk Series: An Update,* GAO-03-119 (Washington, D.C.: January 2003).

[5]GAO-15-290.

identifiable information.[6] In 2018, we updated this high-risk area to reflect the lack of a comprehensive cybersecurity strategy for the federal government.[7] We continued to identify federal information security as a government-wide high-risk area in our most recent high-risk update, issued in March 2019.[8]

My statement today provides an update on agencies' progress in improving the management of IT acquisitions and operations and the nation's cybersecurity. Specifically, our objectives were to summarize our key reports issued since fiscal year 2010 in these areas and assess agencies' progress in implementing our associated recommendations. In particular, we discuss federal agencies' (1) implementation of Chief Information Officer (CIO) responsibilities, (2) fulfillment of CIO IT acquisition review requirements, (3) data center consolidation efforts, (4) management of software licenses, and (5) cybersecurity. More detailed information on our objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Each year, the federal government invests over $90 billion in IT. Nevertheless, we have previously reported that investments in federal IT too often resulted in failed projects that incurred cost overruns and schedule slippages, while contributing little to the desired mission-related outcomes. For example:

[6]Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[7]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[8]GAO-19-157SP.

- The United States Coast Guard (Coast Guard) decided to terminate its Integrated Health Information System project in 2015. As reported by the agency in August 2017, the Coast Guard spent approximately $60 million 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.[10]
- The Department of Defense's Expeditionary Combat Support System was canceled in December 2012 after spending more than a billion dollars and failing to deploy within 5 years of initially obligating funds.[11]
- The Department of Homeland Security's (DHS) Secure Border Initiative Network program was ended in January 2011, after the department obligated more than $1 billion for the program.[12]

Our past work found that these and other failed IT projects often suffered from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance. In many instances, agencies had not consistently applied best practices that are critical to successfully acquiring IT.

[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).

[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).

Federal IT projects have also failed due to a lack of oversight and governance. Executive-level governance and oversight across the government has often been ineffective, specifically from CIOs. For example, we have reported that some CIOs' roles were limited because they did not have the authority to review and approve the entire agency IT portfolio.[13]

In addition to failures when acquiring IT, our cybersecurity work at federal agencies continues to highlight information security deficiencies. The following examples describe the types of risks we have found at federal agencies:

- In May 2020, we reported that, although progress had been made, the Internal Revenue Service had new and continuing information security deficiencies that, collectively, increased the risk of critical operations being disrupted, and of unauthorized access to financial reporting and taxpayer data.[14]
- In September 2018, we reported that the Department of Education's Office of Federal Student Aid had exercised minimal oversight of lenders' protection of student data and lacked assurance that appropriate risk-based safeguards were being effectively implemented, tested, and monitored.[15]
- In August 2017, we issued a report stating that, since the 2015 data breaches, the Office of Personnel Management (OPM) had taken actions to prevent, mitigate, and respond to data breaches involving sensitive personal and background investigation information.[16] However, we noted that the agency had not fully implemented recommendations that DHS's United States Computer Emergency Readiness Team made to OPM to help the agency improve its overall

[13]GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, GAO-11-634 (Washington, D.C.: Sept. 15, 2011).

[14]GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls,* GAO-20-411R (Washington, D.C.: May 13, 2020).

[15]GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information,* GAO-18-518 (Washington, D.C.: Sept. 17, 2018).

[16]GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

security posture and improve its ability to protect its systems and information from security breaches.

- We reported in August 2016 that the information security of the Food and Drug Administration had significant weaknesses that jeopardized the confidentiality, integrity, and availability of its information systems and industry and public health data.[17]

  In May 2016, we found that the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, OPM, and the Department of Veteran Affairs did not always control access to selected high-impact systems, patch known software vulnerabilities, or plan for contingencies. An underlying reason for these weaknesses was that the agencies had not fully implemented key elements of their information security programs.[18]

FITARA Increases CIO Authorities and Responsibilities for Managing IT

Congress and the President have enacted various key pieces of reform legislation to address IT management issues. These include the federal IT acquisition reform legislation commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA).[19] 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.[20] The law includes specific requirements related to seven areas:

- **Agency CIO authority enhancements.** CIOs at covered agencies have the authority to, among other things, (1) approve the IT budget

[17]GAO, *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk,* GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

[18]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems,* GAO-16-501 (Washington, D.C.: May 18, 2016).

[19]*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).

[20]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.

requests of their respective agencies and (2) review and approve IT contracts.

- **Federal data center consolidation initiative (FDCCI).** Agencies covered by FITARA are required, among other things, to provide a strategy for consolidating and optimizing their data centers and issue quarterly updates on the progress made.
- **Enhanced transparency and improved risk management.** The Office of Management and Budget (OMB) and covered agencies are to make detailed information on federal IT investments publicly available, and agency CIOs are to categorize their investments by level of risk.
- **Portfolio review.** Covered agencies are to annually review IT investment portfolios in order to, among other things, increase efficiency and effectiveness and identify potential waste and duplication.
- **Expansion of training and use of IT acquisition cadres.** Covered agencies are to update their 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 (i.e., multi-functional groups of professionals to acquire and manage complex programs), or developing agreements with other agencies that have such cadres.
- **Government-wide software purchasing program.** The General Services Administration is to develop a strategic sourcing initiative to enhance government-wide acquisition and management of software. In doing so, the law requires that, to the maximum extent practicable, the General Services Administration should allow for the purchase of a software license agreement that is available for use by all executive branch agencies as a single user.[21]

[21]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).

- **Maximizing the benefit of the Federal Strategic Sourcing Initiative.**[22] Federal agencies are required to compare their purchases of services and supplies to what is offered under the Federal Strategic Sourcing Initiative.

In June 2015, OMB released guidance describing how agencies are to implement FITARA.[23] This guidance was intended to, among other things:

- assist agencies in aligning their IT resources with statutory requirements;
- establish government-wide IT management controls to meet the law's requirements, while providing agencies with flexibility to adapt to unique agency processes and requirements;
- strengthen the relationship between agency CIOs and bureau CIOs; and
- strengthen CIO accountability for IT costs, schedules, performance, and security.

The guidance identifies a number of actions that agencies are to take to establish a basic set of roles and responsibilities (referred to as the common baseline) for CIOs and other senior agency officials and, thus, to implement the authorities described in the law. For example, agencies are to conduct a self-assessment and submit a plan describing the changes they intend to make to ensure that common baseline responsibilities are implemented.

In addition, in August 2016, OMB released guidance intended to, among other things, define a framework for achieving the data center consolidation and optimization requirements of FITARA.[24] The guidance directed agencies to develop a data center consolidation and optimization strategic plan that defined the agency's data center strategy for fiscal years 2016, 2017, and 2018. This strategy was to include, among other

[22]The Federal Strategic Sourcing Initiative is a program established by the General Services Administration and the Department of the Treasury to address government-wide opportunities to strategically source commonly purchased goods and services and eliminate duplication of efforts across agencies.

[23]OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[24]OMB, *Data Center Optimization Initiative (DCOI),* Memorandum M-16-19 (Washington, D.C.: Aug. 1, 2016).

things, a statement from the agency CIO indicating whether the agency had complied with all data center reporting requirements in FITARA. Further, the guidance states that OMB is to maintain a public dashboard to display consolidation-related costs savings and optimization performance information for the agencies.

In June 2019, OMB issued memorandum M-19-19, which updated the data center optimization initiative and redefined a data center as a purpose-built, physically separate, dedicated space that meets certain criteria.[25] It also revised the priorities for consolidating and optimizing federal data centers. Specifically, OMB directed agencies to report on spaces designed to be data centers (i.e., tiered data centers) as part of their inventories and to focus efforts on data centers that host business applications, rather than special purpose data centers.[26]

In addition, OMB described criteria for designating certain data centers as mission critical facilities, and that would not, therefore, be taken into consideration when setting new agency-specific closure targets.[27] Those mission critical designations are also assumed to be granted unless OMB specifically overturns them. Regarding cost savings, OMB specified in M-19-19 that agency-specific targets would be set in collaboration with each agency and appropriately aligned to that agency's mission and budget.

OMB memorandum M-19-19 also replaced the previous optimization metrics with new measures that focus on reporting the numbers of agencies' virtualized hosts,[28] underutilized servers, and data centers with advanced energy metering, as well as the percentage of time that data centers were expected to be available to provide services.[29] In contrast to

[25]OMB, *Update to Data Center Optimization Initiative (DCOI)*, Memorandum M-19-19 (Washington, D.C.: June 25, 2019).

[26]The term "tiered" and its definition are derived by OMB from the Uptime Institute's Tier Classification System. However, OMB notes that no specific certification is required in order for a data center to be considered tiered by OMB. According to OMB M-16-19, all data centers not marked as tiered were to be considered non-tiered.

[27]For example, mission critical data centers could include primarily weather stations, air traffic control facilities, federal labs, and research facilities. Agencies are to categorize these data centers as "key mission facilities" to exempt them from closure.

[28]A virtual host is a physical machine that uses technology to allow multiple software-based machines with different operating systems to run in isolation side-by-side.

[29]Advanced energy metering and management tools can help agencies accurately measure how efficiently a data center uses energy and track performance over time.

the previous guidance, M-19-19 does not specify government-wide performance targets for the optimization metrics. Instead, OMB worked with agencies to establish agency-specific targets. In addition, the guidance describes how agencies could apply for an optimization performance exemption for data centers where typical optimization activities (consolidation of data collection, storage, and processing to a central location) are technically possible but increase the response time for systems beyond a reasonable limit.

Congress Has Undertaken Efforts to Continue Selected FITARA Provisions and Modernize Federal IT

Congress has recognized the importance of agencies' continued implementation of FITARA provisions, and has taken legislative action to extend selected provisions beyond their original dates of expiration. Specifically, Congress and the President enacted laws to:

- remove the expiration dates for the enhanced transparency and improved risk management provisions, which were set to expire in 2019;
- remove the expiration date for portfolio review, which was set to expire in 2019; and
- extend the expiration date for FDCCI from 2018 to 2020.[30]

In addition, Congress and the President enacted a law in 2017 to authorize the availability of funding mechanisms to help further agencies' efforts to modernize IT. The law, known as the Modernizing Government Technology (MGT) Act, authorizes 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.[31] The law also creates 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.

Further, in February 2018, OMB issued guidance for agencies on implementing the MGT Act.[32] The guidance was intended to provide agencies additional information regarding the Technology Modernization

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

[31]*National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G (2017).

[32]OMB, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

Fund, as well as the administration and funding of the related IT working capital funds. Specifically, the guidance allowed agencies to begin submitting initial project proposals to receive funding for modernization from the Technology Modernization Fund on February 27, 2018. Subsequently, in March 2018, OMB issued funding guidelines for projects receiving awards. The guidelines stated that project proposals must include a reliable estimate of any project-related cost savings or avoidance relative to pre-modernization activities.[33]

In addition, in accordance with the MGT Act, the guidance provided details regarding a Technology Modernization Board, which is to consist of (1) the Federal CIO; (2) a senior IT official from the General Services Administration; (3) a member of DHS's National Protection and Program Directorate;[34] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition that were appointed by the Director of OMB. As of July 2020, the Technology Modernization Board reported that it had awarded $81.48 million to nine projects.

FISMA Establishes Responsibilities for Agencies to Address Federal Cybersecurity

Congress and the President enacted the *Federal Information Security Modernization Act of 2014* (FISMA) to improve federal cybersecurity and clarify government-wide responsibilities.[35] The act addresses the increasing sophistication of cybersecurity attacks, promotes the use of automated security tools with the ability to continuously monitor and diagnose the security posture of federal agencies, and provides for improved oversight of federal agencies' information security programs. To this end, the act clarifies and assigns specific responsibilities to entities such as OMB, DHS, and the federal agencies. Table 1 describes a selection of the OMB, DHS, and agency responsibilities.

[33]OMB, *Funding Guidelines for Agencies Receiving Disbursements from the Technology Modernization Fund* (Washington, D.C.: Mar. 12, 2018).

[34]The National Protection and Program Directorate (NPPD) was the Department of Homeland Security component responsible for addressing physical and cyber infrastructure protection. The Cybersecurity and Infrastructure Security Agency Act of 2018 renames NPPD the Cybersecurity and Infrastructure Security Agency and establishes a Director and responsibilities for the agency.

[35]*The Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this testimony, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

Table 1: Selected Federal Information Security Modernization Act of 2014 (FISMA) Responsibilities

Responsible agency or agencies	FISMA responsibilities
Office of Management and Budget (OMB)	• Develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems. • Require agencies to identify and provide information security protections commensurate with assessments of risk to their information and information systems. • Report annually, in consultation with the Department of Homeland Security (DHS), on the effectiveness of information security policies and practices. • Ensure that data breach notification policies and guidelines are periodically updated and require notification to congressional committees and affected individuals. • Ensure development of guidance for evaluating the effectiveness of an information security program and practices, in consultation with DHS, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties, as appropriate.
DHS	• Consult with OMB to administer the implementation of agency information security policies and practices for non-national security information systems.
Executive branch agencies covered by FISMA	• Develop, document, and implement an agency-wide information security program that includes, among other things, periodic risk assessments, policies and procedures, plans for providing adequate information security, security awareness training, and periodic testing and evaluation. • Ensure that senior officials carry out assigned responsibilities and that all personnel are held accountable for complying with the agency's information security program. • Submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, as well as compliance with the act to OMB, certain congressional committees, and the Comptroller General of the United States. The annual report is to include descriptions of major security incidents.
Executive branch agencies' Office of the Inspector General or independent auditor	• Assess the effectiveness of the agency's information security policies, procedures, and practices.

Source: GAO analysis. | GAO-20-691T

The Administration Has Undertaken Efforts to Improve and Modernize Federal IT and Strengthen Cybersecurity

Beyond the implementation of FITARA, FISMA, and related actions, the administration has also initiated other efforts intended to improve federal IT and the nation's cybersecurity. Specifically, in March 2017, the administration established the Office of American Innovation, which has a mission to, among other things, make recommendations to the President on policies and plans aimed at improving federal government operations and services. In doing so, the office is to consult with both OMB and the Office of Science and Technology Policy on policies and plans intended

to improve government operations and services, improve the quality of life for Americans, and spur job creation.[36]

In May 2017, the Administration also established the American Technology Council, which has a goal of helping to transform and modernize federal agency IT and how the federal government uses and delivers digital services.[37] The President is the chairman of this council, and the Federal CIO and the United States Digital Service Administrator are among the members.[38]

In addition, in May 2017, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*[39] This executive order outlined actions to enhance cybersecurity across federal agencies and critical infrastructure to improve the nation's cyber posture and capabilities against cybersecurity threats. Among other things, the order tasked the Director of the American Technology Council[40] to coordinate a report to the President from the Secretary of DHS, the Director of OMB, and the Administrator of the General Services Administration, in consultation with the Secretary of Commerce, regarding the modernization of federal IT.

In response, the *Report to the President on Federal IT Modernization* was issued in December 2017 and outlined the current and envisioned state of federal IT. The report focused on modernization efforts to improve the security posture of federal IT. Further, it recognized that agencies have attempted to modernize systems but have been stymied by a variety of factors, including resource prioritization, ability to procure services quickly, and technical issues. The report provided multiple

[36]The White House Office of Science and Technology Policy provides the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics.

[37]Exec. Order No. 13794, *Establishment of the American Technology Council*, 82 Fed. Reg. 20811 (May 3, 2017).

[38]The United States Digital Service is an office within OMB which aims to improve the most important public-facing federal digital services.

[39]Exec. Order No. 13800, 82 Fed Reg. 22391 (May 16, 2017).

[40]This position is held by an employee of the Executive Office of the President, as designated by the President.

recommendations intended to address these issues through the modernization and consolidation of networks and the use of shared services to enable future network architectures.

Further, in March 2018, the Administration issued the *President's Management Agenda*, which laid out a long-term vision for modernizing the federal government.[41] The agenda identified three related drivers of transformation—IT modernization; data, accountability, and transparency; and the workforce of the future—that are intended to push change across the federal government.

The Administration also established 14 related Cross-Agency Priority goals, many of which have elements that involve IT.[42] In particular, the Cross-Agency Priority goal on IT modernization stated that modern IT must function as the backbone of how government serves the public in the digital age. This goal established three priorities that are to guide the Administration's efforts to modernize federal IT: (1) enhancing mission effectiveness by improving the quality and efficiency of critical services, including the increased utilization of cloud-based solutions; (2) reducing cybersecurity risks to the federal mission by leveraging current commercial capabilities and implementing cutting edge cybersecurity capabilities; and (3) building a modern IT workforce by recruiting, reskilling, and retaining professionals able to help drive modernization with up-to-date technology.

On May 15, 2018, the President signed Executive Order 13833: *Enhancing the Effectiveness of Agency Chief Information Officers*.[43] Among other things, this executive order was intended to better position agencies to modernize their IT systems, execute IT programs more efficiently, and reduce cybersecurity risks. The order pertains to 22 of the

[41]President's Management Council and Executive Office of the President, *President's Management Agenda* (Washington, D.C.: Mar. 20, 2018).

[42]Cross-Agency Priority goals were established in response to the Government Performance and Results Act Modernization Act of 2010, Sec. 5, Pub. L. No. 111-352 (Jan. 4, 2011); 124 Stat. 3866, 3873; 31 U.S.C. § 1120(a)(1)(B).

[43]Exec. Order No. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*, 83 Fed. Reg. 23345 (May 18, 2018).

24 Chief Financial Officers (CFO) Act agencies; the Department of Defense and the Nuclear Regulatory Commission are exempt.[44]

For the covered agencies, the executive order strengthened the role of agency CIOs by, among other things, requiring them to report directly to their agency head; serve as their agency head's primary IT strategic advisor; and have a significant role in all management, governance, and oversight processes related to IT. In addition, one of the cybersecurity requirements directed agencies to ensure that the CIO works closely with an integrated team of senior executives, including those with expertise in IT, security, and privacy, to implement appropriate risk management measures.

Agencies Need to Address the IT Acquisitions and Operations High-Risk Area

In the March 2019 update to our high-risk series, we reported that agencies still needed to complete significant work related to the management of IT acquisitions and operations.[45] As government-wide spending on IT increases every year, the need for appropriate stewardship of that investment increases as well. However, we pointed out that OMB and federal agencies have not made significant progress since 2017 in taking the steps needed to improve how these financial resources are budgeted and realized. To address this issue, we highlighted the need for OMB and federal agencies to further implement the requirements of federal IT acquisition reforms, including the enhancement of CIO authority.

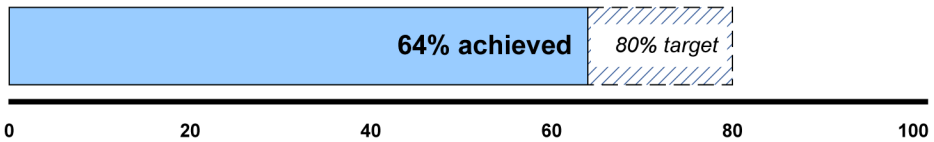
Our update to the IT acquisitions and operations high-risk area also stressed that OMB and agencies needed to continue to implement our prior recommendations in order to improve their ability to effectively and efficiently invest in IT. Specifically, since fiscal year 2010, we have made 1,376 recommendations to OMB and other federal agencies, as well as one matter for Congressional consideration, to address shortcomings in IT acquisitions and operations.

[44]The 24 agencies covered by the CFO Act of 1990, 31 U.S.C. § 901(b) 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.

[45]GAO-19-157SP.

As stated in our 2019 high-risk update, OMB and agencies should demonstrate government-wide progress by, among other things, implementing at least 80 percent of our recommendations related to managing IT acquisitions and operations. As of July 2020, OMB and agencies had fully implemented 880 (or 64 percent) of the 1,376 recommendations. In addition, Congress had addressed the matter for Congressional consideration. Figure 1 summarizes the progress that OMB and agencies had made in addressing our recommendations compared to the 80 percent target.

Figure 1: Summary of the Office of Management and Budget's and Federal Agencies' Progress in Addressing GAO's Information Technology Acquisitions and Operations Recommendations, as of July 2020



Source: GAO analysis of Office of Management and Budget and agency data. | GAO-20-691T

Overall, federal agencies would be better positioned to realize billions in cost savings and additional management improvements if they address these recommendations, including those aimed at implementing CIO responsibilities, reviewing IT acquisitions, improving data center consolidation, and managing software licenses.

Agencies Need to Address Shortcomings and Challenges in Implementing CIO Responsibilities

Laws, such as FITARA, and related guidance assign 35 IT management responsibilities to CIOs in six key areas.[46] These areas are: leadership and accountability, budgeting, information security, investment management, workforce, and strategic planning.

In August 2018, we reported that none of the 24 agencies we reviewed had policies that fully addressed the role of their CIO, as called for by federal laws and guidance.[47] In this regard, a majority of the agencies had fully or substantially addressed the role of their CIOs for the area of

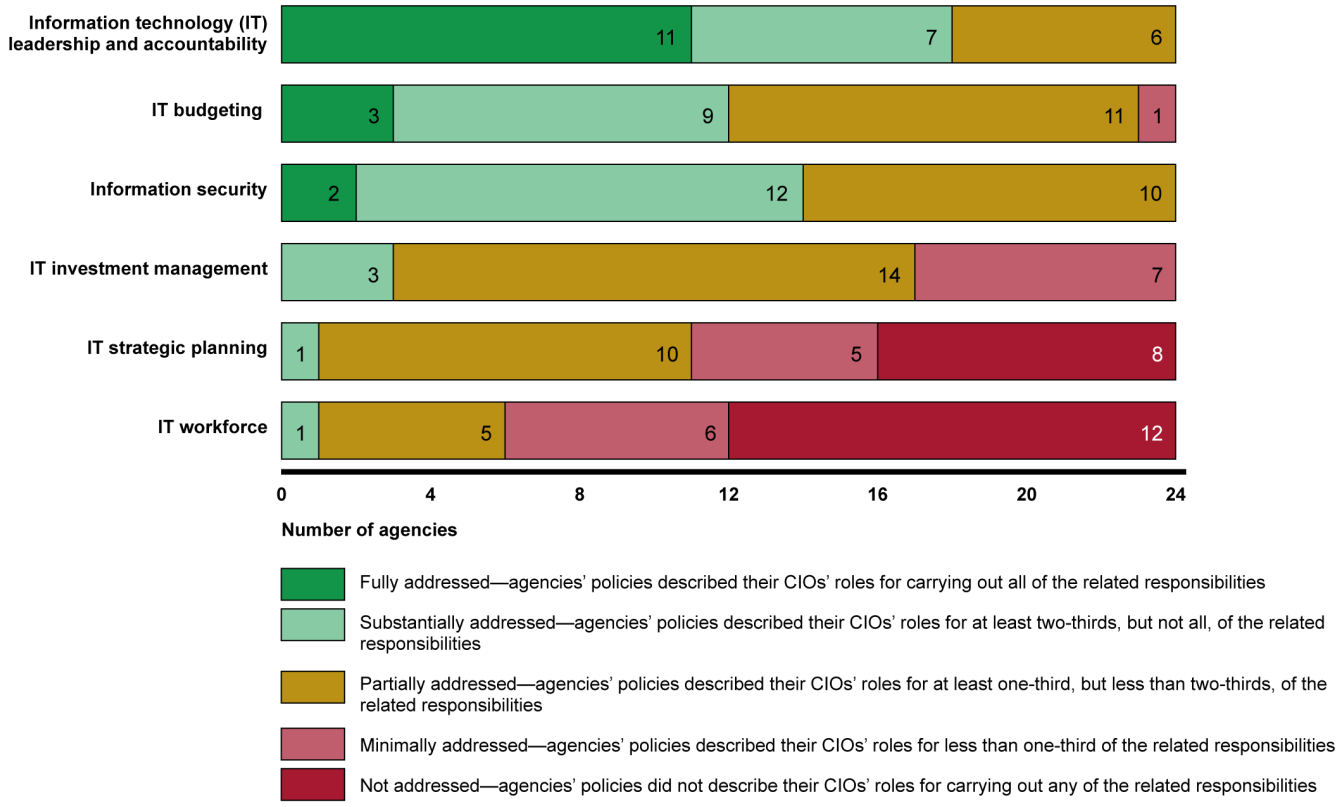
[46]In addition to FITARA, these laws include FISMA (44 U.S.C. § 3554), the Paperwork Reduction Act (44 U.S.C. § 3506), and the Clinger-Cohen Act (40 U.S.C. §§ 11312 and 11313).

[47]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).

leadership and accountability. In addition, a majority of the agencies had substantially or partially addressed the role of their CIOs for two areas: information security and IT budgeting.

However, most agencies had partially or minimally addressed the role of their CIOs for two areas: investment management and strategic planning. Further, the majority of the agencies minimally addressed or did not address the role of their CIOs for the remaining area: IT workforce. Figure 2 depicts the extent to which the 24 agencies had policies that addressed the role of their CIOs for the six areas.

Figure 2: Extent to Which 24 Selected Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO), Presented from Most Addressed to Least Addressed Area, as of August 2018



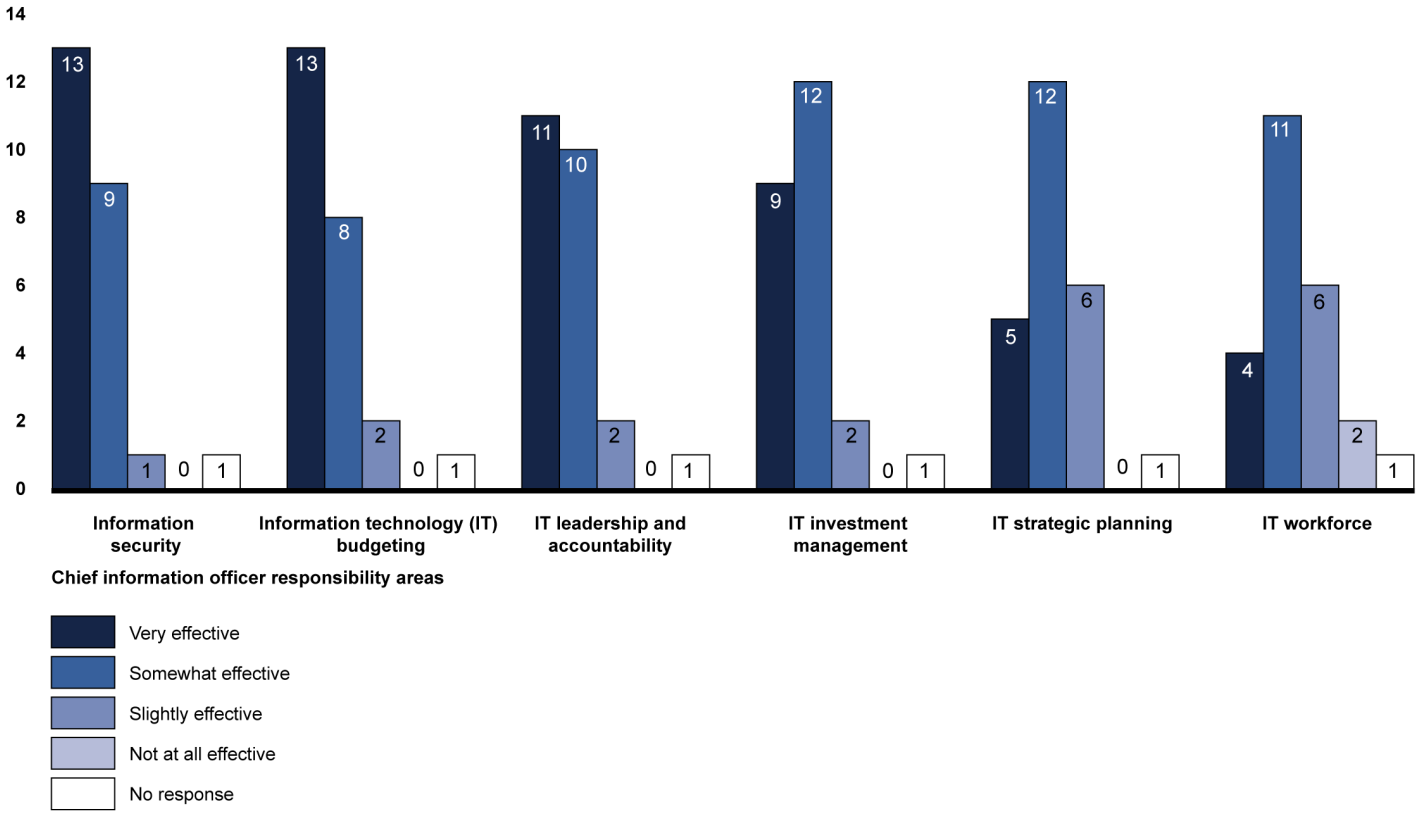
Source: GAO analysis of agency IT management policies. | GAO-20-691T

Notwithstanding the shortfalls in agencies' policies addressing the roles of their CIOs, most agency officials stated that their CIOs are implementing the responsibilities even if the agencies do not have policies requiring implementation.

Nevertheless, in their responses to our survey, the CIOs of the 24 selected agencies acknowledged that they were not always very effective in implementing the six IT management areas. Specifically, at least 10 of the CIOs indicated that they were less than very effective for each of the six areas of responsibility. We believe that until agencies fully address the role of CIOs in their policies, they will be limited in addressing longstanding IT management challenges.

Figure 3 depicts the extent to which the CIOs reported their effectiveness in implementing the six areas of responsibility.

Figure 3: Extent to Which 24 Agency Chief Information Officers (CIO) Reported Effective Implementation of Six Responsibility Areas, Presented from Most Effective to Least Effective Area, as of August 2018



Source: Chief information officer responses to GAO survey. | GAO-20-691T

Beyond the actions of the agencies, however, shortcomings in agencies' policies were also partially attributable to two weaknesses in OMB's guidance. First, the guidance did not comprehensively address all CIO

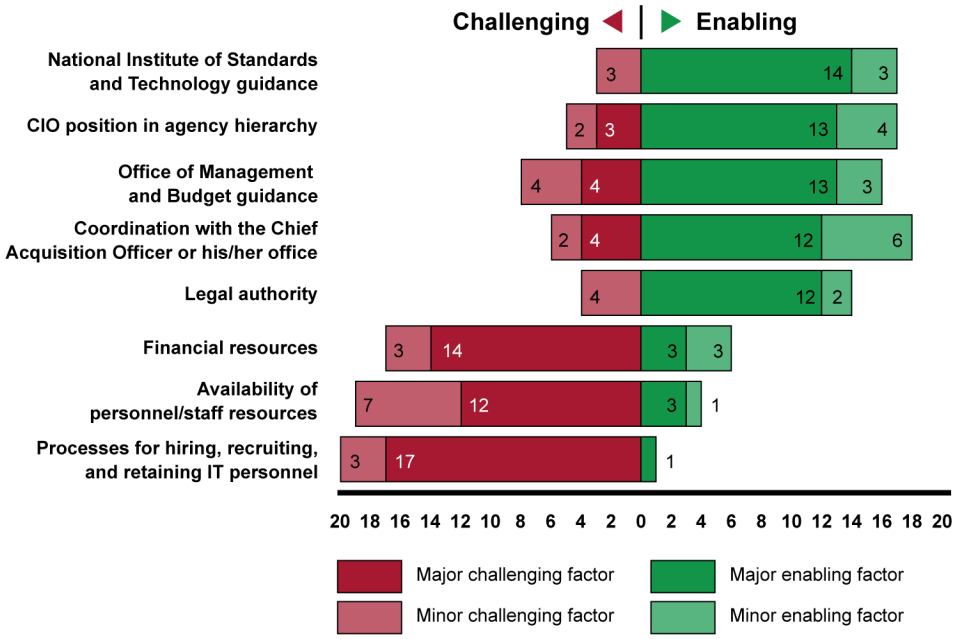
responsibilities, such as those related to assessing the extent to which personnel meet IT management knowledge and skill requirements and ensuring that personnel are held accountable for complying with the information security program. Correspondingly, the majority of the agencies' policies did not fully address nearly all of the responsibilities that were not included in OMB's guidance.

Second, OMB's guidance did not ensure that CIOs had a significant role in (1) IT planning, programming, and budgeting decisions; and (2) execution decisions and the management, governance, and oversight processes related to IT, as required by federal law and guidance. In the absence of comprehensive guidance, CIOs were not positioned to effectively acquire, maintain, and secure their IT systems.

In response to the survey conducted for our August 2018 report, the 24 agency CIOs also identified a number of factors that enabled and challenged their ability to effectively manage IT. Specifically, most agency CIOs cited five factors as being enablers to effectively carrying out their responsibilities: (1) NIST guidance, (2) the CIO's position within the agency hierarchy, (3) OMB guidance, (4) coordination with the Chief Acquisition Officer (CAO), and (5) legal authority. Further, the CIOs cited three factors as major challenges to their ability to effectively carry out responsibilities: (1) processes for hiring, recruiting, and retaining IT personnel; (2) financial resources; and (3) the availability of personnel/staff resources.

As shown in figure 4, the five enabling factors were identified by at least half of the 24 CIOs and the three factors cited as major challenges were identified by at least half of the CIOs.

Figure 4: Factors Commonly Identified as Enabling and Challenging Chief Information Officers (CIO) to Effectively Manage Information Technology (IT), Presented from Most Enabling to Least Enabling Factor



Source: Chief information officer responses to GAO survey. | GAO-20-691T

Although OMB issued guidance aimed at addressing the three factors identified by a majority of the CIOs as major challenges, the guidance did not fully do so. Further, regarding the financial resources challenge, OMB recently required agencies to provide data on CIO authority over IT spending; however, its guidance did not provide a complete definition of that authority. In the absence of such guidance, agencies created varying definitions of CIO authority. Until OMB updates its guidance to include a complete definition of the authority that CIOs are to have over IT spending, it will be difficult for OMB to identify any deficiencies in this area and to help agencies make any needed improvements.

In order to address challenges in implementing CIO responsibilities, we made three recommendations to OMB and one recommendation to each of the 24 selected federal agencies (related to each of the six IT management areas). Most agencies agreed with or had no comments on the recommendations. However, as of July 2020, only four of the 27 total recommendations had been implemented. We will continue to monitor the implementation of these recommendations.

Agencies Need to Ensure That IT Acquisitions Are Reviewed and Approved by CIOs

FITARA includes a provision to enhance covered agency CIOs' authority through, among other things, requiring agency heads to ensure that CIOs review and approve IT contracts. OMB's FITARA implementation guidance expanded upon this aspect of the legislation in a number of ways.[48] Specifically, according to the guidance:

- CIOs may review and approve IT acquisition strategies and plans, rather than individual IT contracts;[49]
- CIOs can designate other agency officials to act as their representatives, but the CIOs must retain accountability;[50]
- CAOs are responsible for ensuring that all IT contract actions are consistent with CIO-approved acquisition strategies and plans; and
- CAOs are to indicate to the CIOs when acquisition strategies and acquisition plans include IT.

In January 2018, we reported[51] that most of the CIOs at 22 selected agencies were not adequately involved in reviewing billions of dollars of IT acquisitions.[52] For instance, most of the 22 agencies did not identify all of their IT contracts. In this regard, the agencies identified 78,249 IT-related contracts, to which they obligated $14.7 billion in fiscal year 2016. However, we identified 31,493 additional IT contracts with combined obligations totaling $4.5 billion, raising the total amount obligated to IT contracts by these agencies in fiscal year 2016 to at least $19.2 billion.

[48]OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

[49]OMB's guidance states that CIOs should only review and approve individual IT contract actions if they are not part of an approved acquisition strategy or plan.

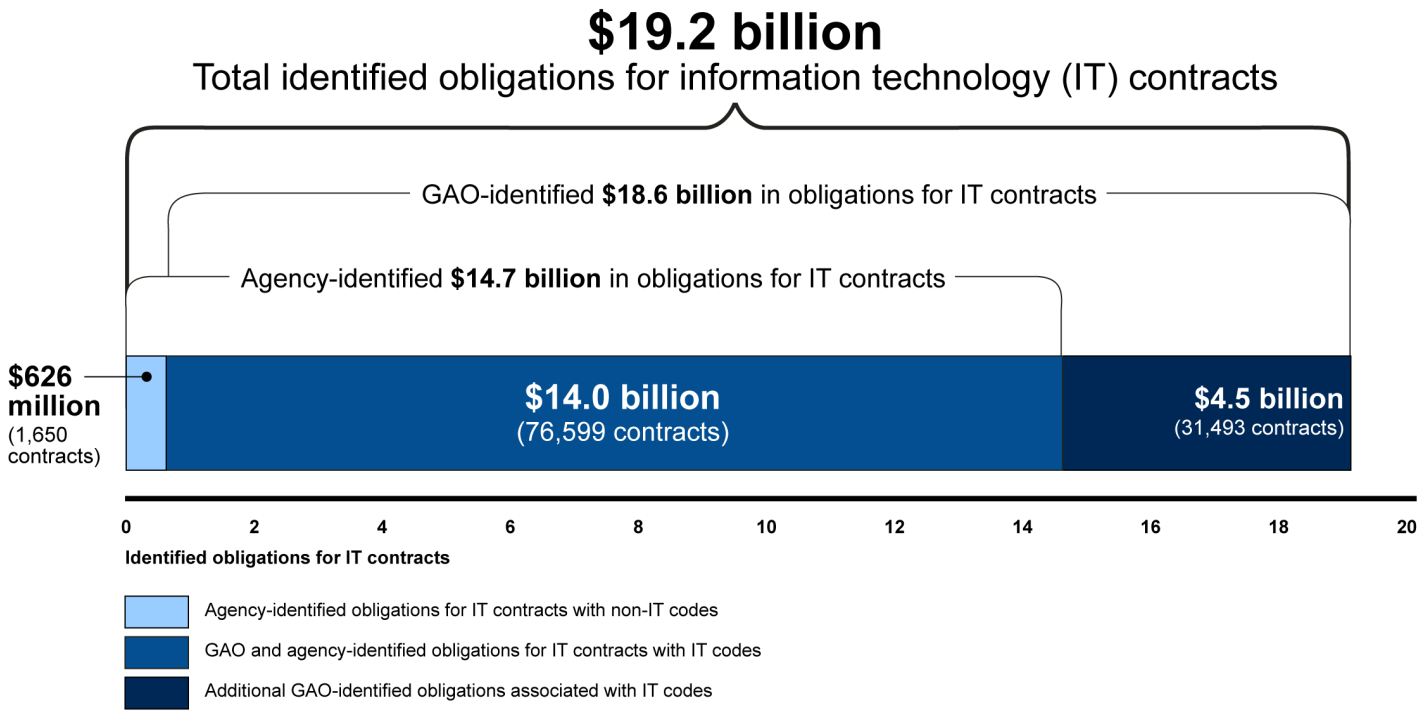
[50]OMB has interpreted FITARA's "governance process" provision to permit such delegation. That provision allows covered agencies to use the governance processes of the agency to approve a contract or other agreement for IT if the CIO of the agency is included as a full participant in the governance process.

[51]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).

[52]The 22 agencies were the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, 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.

Figure 5 reflects the obligations that the 22 selected agencies reported to us relative to the obligations we identified.

Figure 5: Agency- and GAO-Identified Approximate Dollars Obligated to Fiscal Year 2016 IT Contracts at 22 Selected Agencies



Source: GAO analysis of agency and USAspending.gov data. | GAO-20-691T

Note: Due to rounding, the totals may not equal the sum of component obligation amounts.

The percentage of additional IT contract obligations we identified varied among the selected agencies. For example, the Department of State did not identify 1 percent of its IT contract obligations. Conversely, eight agencies did not identify over 40 percent of their IT contract obligations.

Many of the selected agencies that did not identify these IT contract obligations also did not follow OMB guidance. Specifically, 14 of the 22 agencies did not involve the acquisition office in their process to identify IT acquisitions for CIO review, as required by OMB. In addition, seven agencies did not establish guidance to aid officials in recognizing IT. We concluded that, until these agencies involve the acquisition office in their IT acquisition identification processes and establish supporting guidance, they cannot ensure that they will identify all such acquisitions. Without

proper identification of IT acquisitions, these agencies and their CIOs cannot effectively provide oversight of the acquisitions.

In addition to not identifying all IT contracts, 14 of the 22 selected agencies did not fully satisfy OMB's requirement that the CIO review and approve IT acquisition plans or strategies. Further, only 11 of 96 randomly selected IT contracts at 10 of the 22 agencies were CIO-reviewed and approved as required by OMB's guidance. The 85 contracts that were not reviewed had a total possible value of approximately $23.8 billion.

Until agencies ensure that CIOs are able to review and approve all IT acquisitions, CIOs will continue to have limited visibility and input into their agencies' planned IT expenditures and will not be able to effectively use the increased authority that FITARA's contract approval provision is intended to provide. Further, agencies will likely miss an opportunity to strengthen their CIOs' authority and the oversight of acquisitions. As a result, agencies may award IT contracts that are duplicative, wasteful, or poorly conceived.

As a result of these findings, we made 39 recommendations in our January 2018 report. Among these, we recommended that agencies ensure that their acquisition offices are involved in identifying IT acquisitions and issuing related guidance, and that IT acquisitions are reviewed in accordance with OMB guidance. OMB and the majority of the agencies generally agreed with or did not comment on the recommendations. As of July 2020, 29 of the 39 recommendations had been implemented. Implementing the remaining 10 recommendations can help strengthen CIOs' authority and improve the oversight and management of IT contracts. We will continue to monitor the implementation of the remaining recommendations.

Agencies Have Made Significant Progress in Consolidating Data Centers, but Need to Take Action to Achieve Planned Cost Savings

Data center consolidation efforts are key to implementing FITARA. Specifically, OMB established the FDCCI in February 2010 to improve the efficiency, performance, and environmental footprint of federal data center activities. The enactment of FITARA in 2014 codified and expanded the initiative.

In addition, OMB's August 2016 memorandum that established the Data Center Optimization Initiative (DCOI) included guidance on how to implement the data center consolidation and optimization provisions of

FITARA.[53] Among other things, the guidance required agencies to consolidate inefficient infrastructure, optimize existing facilities, improve their security posture, and achieve cost savings.[54]

According to the 24 agencies covered by the initiative, data center consolidation and optimization efforts resulted in approximately $4.7 billion in cost savings from fiscal years 2012 through 2019. Even so, additional work remains to fully carry out the initiative. Specifically, in a series of reports that we issued from July 2011 through March 2020, we noted that, while data center consolidation could potentially save the federal government billions of dollars, weaknesses existed in several areas, including agencies' data center consolidation plans and data center optimization, and in OMB's tracking and reporting on related cost savings.[55]

Most recently, we reported in March 2020 that the 24 agencies covered by the initiative had reported progress toward achieving OMB's fiscal year 2019 goals for closing unneeded data centers.[56] Specifically, 23 agencies reported 102 fiscal year 2019 data center closures through August 31, 2019, with an additional 184 planned closures by the end of fiscal year

[53]OMB, Memorandum M-16-19.

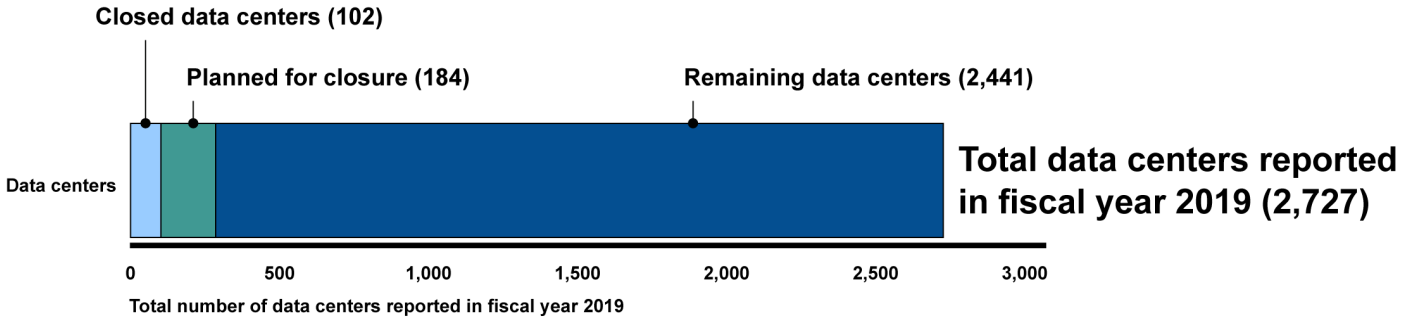
[54]In June 2019, OMB issued Memorandum M-19-19, which updated the data center optimization initiative and redefined a data center as a purpose-built, physically separate, dedicated space that meets certain criteria. It also revised the priorities for consolidating and optimizing federal data centers. We have ongoing work reviewing these changes.

[55]GAO, *Data Center Optimization: Agencies Report Progress, but Oversight and Cybersecurity Risks Need to Be Addressed,* GAO-20-279 (Washington, D.C.: Mar. 5, 2020); *Data Center Optimization: Additional Agency Actions Needed to Meet OMB Goals,* GAO-19-241 (Washington, D.C.: Apr. 11, 2019); *Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations*, GAO-18-264 (Washington, D.C.: May 23, 2018); *Data Center Optimization: Agencies Need to Address Challenges and Improve Progress to Achieve Cost Savings Goal,* GAO-17-448 (Washington, D.C.: Aug. 15, 2017); *Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*, GAO-17-388 (Washington, D.C.: May 18, 2017); *Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established [Reissued on March 4, 2016],* GAO-16-323 (Washington, D.C.: Mar. 3, 2016); *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings,* GAO-14-713 (Washington, D.C.: Sept. 25, 2014); *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal,* GAO-13-378 (Washington, D.C.: Apr. 23, 2013); *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed,* GAO-12-742 (Washington, D.C.: July 19, 2012); and *Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings,* GAO-11-565 (Washington, D.C.: July 19, 2011).

[56]GAO-20-279.

2019. Regarding the remaining data centers, agencies also reported plans to close at least 37 starting in fiscal year 2020. Figure 6 shows the 2,727 data centers agencies reported in fiscal year 2019, as well as the progress agencies have made in their efforts to close 286 of those data centers.

Figure 6: Total Number of Federal Data Centers Closed, Planned for Closure, or Not Planned for Closure for Fiscal Year 2019, as of August 31, 2019, as Reported by the Agencies



Source: GAO analysis of agency data. | GAO-20-691T

As previously noted, OMB narrowed the scope of the type of facilities that would be defined as a data center in its June 2019 memorandum M-19-19. As a result, agencies are no longer required to report on approximately 2,000 facilities, some of which are considerable in size and will continue to operate. Further, many of the smaller facilities that are exempted from DCOI reporting are the types of data centers that OMB has stated in the past should be included in DCOI because of the risks they posed. Because of OMB's decision to remove these types of facilities from DCOI reporting, agencies may lose track of the security vulnerabilities that these facilities present due to the consequent reduction in overall visibility and oversight into all data centers.

In addition, the 24 agencies reported progress against three of OMB's data center optimization metrics as described in memorandum M-19-19.[57] Specifically, these metrics focus on reporting the numbers of agencies' virtualized hosts, underutilized servers, and data centers with advanced energy metering. As of September 2019, eight agencies reported that they had met all three targets for the metrics, five reported having met two targets, and six reported having met one target. In addition, one agency

[57]For the fourth metric from M-19-19 (data center availability), the data were not sufficiently reliable to report on because of unexpected variances in the information reported by the agencies.

had not established any targets, and four agencies reported that they no longer owned any data centers.

While the definitions for the three revised metrics included the key characteristics of being clearly defined and objective, they did not fully include all of the information that would enable a determination of progress against goals. Specifically, these metrics call for counts of the actual numbers of (1) virtualized servers, (2) data centers with advanced energy metering, and (3) underutilized servers. However, the metrics do not include a count of the entire universe of servers and data centers. Lacking this information, percentages cannot be calculated to determine progress. For instance, if the number of an agency's virtualized servers increased at the same time that the universe of servers expanded at an even higher rate, then the agency's progress would actually be negative.

Of the 24 agencies, 23 reported in August 2019 that they had met, or planned to meet, OMB's fiscal year 2019 savings goal of $241.5 million. One agency did not complete a plan, but indicated that it intended to do so in the future. Agencies also reported plans to save about $264 million in fiscal year 2020.

From July 2011 through March 2020, we made a total of 204 recommendations to OMB and the 24 agencies to improve the execution and oversight of the initiative. Most agencies and OMB agreed with our recommendations or had no comments. As of July 2020, 133 of these 204 recommendations had been implemented. Implementing the remaining recommendations could yield additional cost savings for agencies.

Agencies Have Improved Management of Software Licenses

In our 2015 high-risk report's discussion of IT acquisitions and operations, we identified the management of software licenses as a focus area, in part because of the potential for cost savings. Federal agencies engage in thousands of software licensing agreements annually. The objective of software license management is to manage, control, and protect an organization's software assets. Effective management of these licenses can help avoid purchasing too many licenses, which can result in unused software, as well as too few licenses, which can result in noncompliance with license terms and cause the imposition of additional fees.

As part of its PortfolioStat initiative, OMB has developed a policy that addresses software licenses.[58] This policy requires agencies to conduct an annual, agency-wide IT portfolio review to, among other things, reduce commodity IT spending. Such areas of spending could include software licenses.

In May 2014, we reported on federal agencies' management of software licenses and determined that better management was needed to achieve significant savings government-wide.[59] Of the 24 selected agencies we reviewed, only two had comprehensive policies that included the establishment of clear roles and central oversight authority for managing enterprise software license agreements, among other things. Of the remaining 22 agencies, 18 had policies that were not comprehensive, and four had not developed any policies.

Further, we found that only two of the 24 selected agencies had established comprehensive software license inventories, a leading practice that would help them to adequately manage their software licenses. The inadequate implementation of this and other leading practices in software license management was partially due to weaknesses in agencies' policies. As a result, we concluded that agencies' oversight of software license spending was limited or lacking, thus, potentially leading to missed savings. However, the potential savings could be significant considering that, in fiscal year 2012, one major federal agency reported saving approximately $181 million by consolidating its enterprise license agreements, even when its oversight process was ad hoc.

Accordingly, we recommended that OMB issue a directive to help guide agencies in managing software licenses. We also made 135 recommendations to the 24 agencies to improve their policies and practices for managing licenses. Among other things, we recommended that the agencies (1) regularly track and maintain a comprehensive inventory of software licenses and (2) analyze the inventory to identify

[58]In March 2012, OMB launched PortfolioStat, which required agencies to conduct annual reviews of their IT investments and make decisions on eliminating duplication, among other things. In March 2013, OMB launched the second iteration of PortfolioStat with the goal of eliminating duplication and achieving savings through specific actions and time frames.

[59]GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide,* GAO-14-413 (Washington, D.C.: May 22, 2014).

opportunities to reduce costs and better inform investment decision making.

Most agencies generally agreed with the recommendations or had no comments. As of July 2020, all but 12 of the 135 recommendations had been implemented. In particular, for our recommendations on maintaining and analyzing a comprehensive inventory of software licenses, agencies had fully implemented 46 out of 48 recommendations. Implementing the remaining 12 recommendations could further reduce software license spending and duplication. Table 2 reflects the extent to which the 24 agencies implemented the recommendations in these two areas.

Table 2: Federal Agencies' Implementation of GAO's Software License Management Recommendations, as of July 2020

Agency	Tracks and maintains a comprehensive inventory	Uses inventory to make decisions and reduce costs
Department of Agriculture	●	●
Department of Commerce	●	●
Department of Defense	●	●
Department of Education	●	●
Department of Energy	●	●
Department of Health and Human Services	●	●
Department of Homeland Security	●	●
Department of Housing and Urban Development	●	●
Department of Justice	●	●
Department of Labor	●	●
Department of State	●	●
Department of the Interior	●	●
Department of the Treasury	●	●
Department of Transportation	●	●
Department of Veterans Affairs	●	●
Environmental Protection Agency	●	●
General Services Administration	●	●
National Aeronautics and Space Administration	●	●
Nuclear Regulatory Commission	●	●
National Science Foundation	●	●
Office of Personnel Management	◐	◐
Small Business Administration	●	●
Social Security Administration	●	●
U.S. Agency for International Development	●	●

Key:

● Fully—the agency provided evidence that it fully addressed this recommendation

◐ Partially—the agency had plans to address this recommendation

Source: GAO analysis. | GAO-20-691T

Agencies Need to Address Shortcomings in Cybersecurity

Safeguarding federal computer systems has been a longstanding concern. This year marks the 23rd anniversary of GAO's first designation of information security as a government-wide high-risk area in 1997.[60]

As we have previously noted, in order to strengthen the federal government's cybersecurity posture, agencies should fully implement the information security programs required by FISMA. In this regard, FISMA provides a framework for ensuring the effectiveness of information security controls for federal information resources. The law requires each agency to develop, document, and implement an agency-wide information security program. Such a program should include risk assessments; the development and implementation of policies and procedures to cost-effectively reduce risks; plans for providing adequate information security for networks, facilities, and systems; security awareness and specialized training; the testing and evaluation of the effectiveness of controls; the planning, implementation, evaluation, and documentation of remedial actions to address information security deficiencies; procedures for detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations.

Our prior work has identified four major cybersecurity challenges facing the nation. These challenges relate to (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) the security of federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[61]

Since fiscal year 2010, we have made 3,409 recommendations to agencies, as well as three matters for Congressional consideration, aimed at addressing these four cybersecurity challenges. These recommendations have identified actions for agencies to take to strengthen technical security controls over their computer networks and systems. They also have included recommendations for agencies to fully implement aspects of their information security programs, as mandated by FISMA.

Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part, because many of these recommendations have not been implemented. As of July 2020, agencies had fully implemented 2,695 (or 79 percent) of the 3,409

[60]GAO-HR-97-1 and GAO-HR-97-9.

[61]GAO-18-622.

recommendations. In addition, Congress had addressed one of the three matters for Congressional consideration. Until our recommendations are addressed and actions are taken to address the four challenges we identified, the federal government, the nation's critical infrastructures, and the personal information of U.S. citizens will be increasingly susceptible to the existing multitude of cyber-related threats.

Agencies' Inspectors General Are to Identify Information Security Program Weaknesses

In order to determine the effectiveness of the agencies' information security programs and practices, FISMA requires federal agencies' inspectors general to conduct annual independent evaluations. The agencies are to report the results of these evaluations to OMB, and OMB is to summarize the results in annual reports to Congress.

In these evaluations, the inspectors general are to frame the scope of their analyses, identify key findings, and detail recommendations to address the findings. The evaluations also are to capture maturity model ratings for their respective agencies.

Toward this end, in fiscal year 2017, the inspector general community, in partnership with OMB and DHS, finalized a 3-year effort to create a maturity model for FISMA metrics. The maturity model aligns with the five function areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): identify, protect, detect, respond, and recover.[62] This alignment is intended to help promote consistent and comparable metrics and criteria and provide agencies with a meaningful independent assessment of their information security programs.

The maturity model is designed to summarize the status of agencies' information security programs on a five-level capability maturity scale. The five maturity levels are defined as follows:

- Level 1 (Ad hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
- Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.

[62]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: Feb. 12, 2014). NIST issued version 1.1 of the Cybersecurity Framework on April 16, 2018.

- Level 3 (Consistently Implemented): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
- Level 4 (Managed and Measurable): Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
- Level 5 (Optimized): Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

According to this maturity model, Level 4 (managed and measurable) represents an effective level of security for each core function.[63] Therefore, if an inspector general rates three or more of the agency's core security functions at Level 4 or Level 5, then the inspector general can consider that agency to have an effective information security program. However, the inspector general has the discretion to have a different conclusion on program effectiveness if he or she deems it appropriate to do so.

For fiscal year 2019, inspectors general for the 23 civilian CFO Act agencies reported that three of their agencies had effective identify functions, five had effective protect functions, five had effective detect functions, and nine had effective respond functions. Only one inspector general reported that activities comprising its agency's recover function were effective. Table 3 shows the individual maturity ratings for each covered agency.

[63]NIST defines security control effectiveness as the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the information system and are in compliance with established security policies.

Table 3: Inspector General Maturity-Level Ratings of Civilian Federal Agencies' Information Security Policies, Procedures, and Practices Related to the Five Core Security Functions, as of Fiscal Year 2019

Agency	Identify	Protect	Detect	Respond	Recover
Department of Agriculture	2	2	2	4	2
Department of Commerce	2	2	2	2	2
Department of Education	2	2	2	2	3
Department of Energy	3	3	2	3	2
Department of Health and Human Services	3	3	3	3	2
Department of Homeland Security	1	4	1	1	3
Department of Housing and Urban Development	2	2	2	2	3
Department of Justice	3	3	3	4	3
Department of Labor	3	4	3	3	3
Department of State	2	2	1	4	2
Department of the Interior	3	4	4	3	3
Department of the Treasury	3	3	3	3	3
Department of Transportation	2	2	2	2	2
Department of Veterans Affairs	2	2	2	4	3
Environmental Protection Agency	3	3	3	3	3
General Services Administration	4	4	4	4	3
National Aeronautics and Space Administration	2	2	2	3	2
National Science Foundation	3	3	4	3	3
Nuclear Regulatory Commission	4	4	4	4	4
Office of Personnel Management	1	3	2	4	2
Small Business Administration	3	2	2	4	3
Social Security Administration	2	2	2	2	2
U.S. Agency for International Development	4	2	4	4	3

Key:

The five maturity levels, from the least to the most mature, are: Level 1 (Ad hoc); Level 2 (Defined); Level 3 (Consistently Implemented); Level 4 (Managed and Measurable); and Level 5 (Optimized).

Source: GAO analysis of agency fiscal year 2019 Federal Information Security Modernization Act of 2014 reports. | GAO-20-691T

OMB Requires Agencies to Meet Targets for Cybersecurity Metrics

In its efforts toward strengthening the federal government's cybersecurity, OMB also requires agencies to submit related cybersecurity metrics as part of its Cross-Agency Priority goals. In particular, OMB developed a goal so that federal agencies will be able to build and maintain more modern, secure, and resilient IT. A key part of this goal is to reduce cybersecurity risks to the federal mission through three strategies: limit personnel access, manage asset security, and protect networks and data. The key targets supporting each of these strategies correspond to areas

within the FISMA metrics. Table 4 outlines the strategies, their associated targets, and the 23 civilian CFO Act agencies' progress in meeting those targets, as of June 2020.

Table 4: Civilian Agencies' Progress in Meeting the Office of Management and Budget's (OMB) Targets to Reduce Cybersecurity Risks, as Reported by OMB as of June 2020

Strategies to reduce cybersecurity risks	OMB's target(s)	Number of civilian agencies meeting the target (out of 23 agencies)
Limit Personnel Access	**Privileged Network Access Management:** 100 percent of privileged users are required to use a personal identity verification (PIV) card or Authenticator Assurance Level 3 (AAL3) multifactor authentication method to access the agency's network.	18
	High Value Asset (HVA) Access Management: 90 percent of High Value Assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	15
	Automated Access Management: 95 percent of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	19
Manage Asset Security	**Hardware Asset Management:** 95 percent of the organization's unclassified network has implemented a technology solution to detect and alert upon the connection of unauthorized hardware assets.	17
	Software Asset Management: 95 percent of the organization's assets are covered by a capability that is able to detect unauthorized software and alert appropriate security personnel.	17
	Authorization Management: 100 percent of high and moderate impact systems are covered by a valid security authorization to operate.	13
	Mobile Device Management: 95 percent of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	22
Protect Networks and Data	**Intrusion Detection and Prevention:** At least four of six intrusion prevention metrics have met an implementation target of at least 90 percent and 100 percent of email traffic is analyzed using domain-based message authentication, reporting, and conformance email authentication protocols.	16
	Exfiltration and Enhanced Defenses: 90 percent of outbound communications traffic is checked at the external boundaries to detect potential unauthorized exfiltration of information.	20
	Data Protection: At least four of six data protection metrics have met an implementation target of at least 90 percent.	16

Source: GAO summary of Office of Management and Budget data. | GAO-20-691T

In summary, by addressing the high-risk areas on improving the management of IT acquisitions and operations and ensuring the cybersecurity of the nation, the government has the opportunity to both save billions of dollars and advance the efficiency and effectiveness of government services. Most agencies have taken steps to execute key IT management and cybersecurity requirements and initiatives, including implementing CIO responsibilities, requiring CIO reviews of IT acquisitions, realizing data center consolidation cost savings, managing software assets, and complying with FISMA requirements. The agencies

have also continued to address the recommendations that we have made over the past several years. Nevertheless, further efforts by OMB and federal agencies to implement our previous recommendations would better position them to improve the management and security of federal IT. To help ensure that these efforts succeed, we will continue to monitor agencies' efforts toward implementing the recommendations.

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 Carol C. Harris, Director of Information Technology Management Issues, at (202) 512-4456 or harriscc@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 Kevin Walsh (Assistant Director), Meredith Raymond (Analyst-in-Charge), Hannah Brookhart, Chris Businsky, Rebecca Eyler, and Andrew Stavisky.