United States Government Accountability Office

Testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

INFORMATION TECHNOLOGY

Implementation of Recommendations Is Needed to Strengthen Acquisitions, Operations, and Cybersecurity

Accessible Version

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

For Release on Delivery Expected at 10:00 a.m. ET
Wednesday, December 12, 2018

December 12, 2018

GAO Highlights

Highlights of GAO-19-275T, a testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

INFORMATION TECHNOLOGY

Implementation of Recommendations Is Needed to Strengthen Acquisitions, Operations, and Cybersecurity

Why GAO Did This Study

The federal government planned to invest more than $96 billion in IT in fiscal year 2018. However, IT investments have often failed or contributed little to mission-related outcomes. Further, increasingly sophisticated threats and frequent cyber incidents underscore the need for effective information security. As a result, GAO added two areas to its high-risk list: cybersecurity in 1997 and the management of IT acquisitions and operations in 2015.

This statement summarizes federal agencies' progress in improving the management, and ensuring the security, of federal IT. It is primarily based on GAO's reports issued between February 1997 and August 2018 (and an ongoing review) on (1) CIO responsibilities, (2) agency CIOs' involvement in approving IT contracts, (3) data center consolidation efforts, (4) the management of software licenses, and (5) compliance with cybersecurity requirements.

What GAO Recommends

Since fiscal year 2010, GAO has made 1,242 recommendations to OMB and agencies to address shortcomings in IT acquisitions and operations. Since fiscal year 2010, GAO also has made over 3,000 recommendations to federal agencies to improve the security of federal systems. These recommendations include those to improve the implementation of CIO responsibilities, the oversight of the data center consolidation initiative, software license management efforts, and the strength of security programs and technical controls. Most agencies agreed with the recommendations, and GAO will continue to monitor their implementation.

View GAO-19-275T. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

The Office of Management and Budget (OMB) and federal agencies have taken steps to improve the management of information technology (IT) acquisitions and operations and ensure federal cybersecurity through a series of initiatives. As of November 2018, agencies had fully implemented about 59 percent of the 1,242 IT management-related recommendations that GAO has made since fiscal year 2010. Likewise, agencies had implemented about 73 percent of the approximately 3,000 security-related recommendations that GAO has made since 2010. Even with this progress, significant actions remain to be completed.

- **Chief Information Officer (CIO) responsibilities**. Laws such as the Federal Information Technology Acquisition Reform Act (FITARA) and related guidance assigned 35 key IT management responsibilities to CIOs to help address longstanding challenges. However, in August 2018, GAO reported that none of the 24 selected agencies had policies that fully addressed the role of their CIO, as called for by laws and guidance. GAO recommended that OMB and each of the 24 agencies take actions to improve the effectiveness of CIOs' implementation of their responsibilities. As of November 2018, none of the 27 recommendations had been implemented.
- **IT contract approval**. 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. Consequently, GAO made 39 recommendations to improve CIO oversight over these acquisitions. As of November 2018, 27 of the recommendations had not been addressed.
- **Consolidating data centers**. OMB launched an initiative in 2010 to reduce data centers. According to agencies, data center consolidation and optimization efforts have resulted in approximately $4.5 billion in cost savings through 2018. Even so, additional work remains. GAO has made 160 recommendations to OMB and agencies to improve the reporting of related cost savings and to achieve optimization targets. However, as of November 2018, 47 of the recommendations had not been fully addressed.
- **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. As of December 2018, 27 of the recommendations had not been implemented.
- **Improving the security of federal IT systems**. While the government has acted to protect federal information systems, agencies need to improve security programs, cyber capabilities, and the protection of personally identifiable information. The approximately 3,000 recommendations that GAO has made to agencies since 2010 were aimed at improving the security of federal systems and information. Specifically, these recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. As of November 2018, 688 of the security-related recommendations had not been implemented.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees:

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 security of federal information and IT. 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 February 2017, we noted 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 identifiable information.[6] We continued to identify federal information

[1]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[2]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[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.

[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.

security as a government-wide high-risk area in our February 2017 high-risk update report.[7]

My statement today provides an update on agencies' progress in improving the management of IT acquisitions and operations and the security of federal IT. The statement is based on our prior reports issued between February 1997 and August 2018 that 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) compliance with federal cybersecurity requirements. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

In addition, we have included preliminary results from our ongoing work reviewing the progress being made by federal agencies on data center optimization. The draft report related to this work is currently being reviewed by the agencies and we expect to issue it in early 2019.

We conducted the work upon 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

According to the President's budget, the federal government planned to invest more than $96 billion for IT in fiscal year 2018—the largest amount ever budgeted. Despite such large IT expenditures, 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:

- The tri-agency[8] National Polar-orbiting Operational Environmental Satellite System was disbanded in February 2010 at the direction of

[7]GAO-17-317.

the White House's Office of Science and Technology Policy after the program spent 16 years and almost $5 billion.[9]

- 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.[10]
- 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.[11]
- 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.[12]
- 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

[8]The weather satellite program was jointly managed by the National Oceanic and Atmospheric Administration, the Department of Defense, and the National Aeronautics and Space Administration.

[9]See, for example, GAO, *Polar-Orbiting Environmental Satellites: With Costs Increasing and Data Continuity at Risk, Improvements Needed in Tri-agency Decision Making*, GAO-09-564 (Washington, D.C.: June 17, 2009) and *Environmental Satellites: Polar-Orbiting Satellite Acquisition Faces Delays; Decisions Needed on Whether and How to Ensure Climate Data Continuity*, GAO-08-518 (Washington, D.C.: May 16, 2008).

[10]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).

[11]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).

[12]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).

$60 million over 7 years on this project, which resulted in no equipment or software that could be used for future efforts.[13]

Our past work has 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.

Such 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.[14]

In addition to failures when acquiring IT, security deficiencies can threaten systems. As we previously reported, in order to counter security threats, the 23 civilian Chief Financial Officers (CFO) Act agencies spent a combined total of approximately $4 billion on IT security-related activities in fiscal year 2016.[15] Even so, 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 September 2018, we reported that the Department of Education's Office of Federal Student Aid exercises minimal oversight of lenders'

[13]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).

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

[15] The agencies included were the others covered by the CFO Act of 1990, 31 U.S.C. § 901(b): the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, 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 the U.S. Agency for International Development. See GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017). According to the Department of Defense, at the time of our review, the department had not submitted its FISMA report, nor was it required to issue a financial report for fiscal year 2016.

protection of student data and lacks assurance that appropriate risk-based safeguards are being effectively implemented, tested, and monitored.[16]

- In August 2017, we reported 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.[17] However, we noted that the agency had not fully implemented recommendations made to OPM by DHS's United States Computer Emergency Readiness Team to help the agency improve its overall security posture and improve its ability to protect its systems and information from security breaches.
- In July 2017, we reported that information security at the Internal Revenue Service had weaknesses that limited its effectiveness in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer data. An underlying reason for these weaknesses was that the Internal Revenue Service had not effectively implemented elements of its information security program.[18]
- In May 2016, we reported 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, and plan for contingencies. An underlying reason for these weaknesses was that the agencies had not fully implemented key elements of their information security programs.[19]
- In August 2016, we reported that the information security of the Food and Drug Administration had significant weaknesses that jeopardized

[16]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).

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

[18]GAO, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data*, GAO-17-395 (Washington, D.C.: July 26, 2017).

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

the confidentiality, integrity, and availability of its information systems and industry and public health data.[20]

[20]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).

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).[21] 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.[22] 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 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.

[21] *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).

[22] The provisions apply to the agencies covered by the CFO 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, parts of FITARA do not apply to the Department of Defense.

- **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.[23]
- **Maximizing the benefit of the Federal Strategic Sourcing Initiative.**[24] 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.[25] This guidance is 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

[23]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).

[24]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.

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

- 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.[26] 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 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.

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

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

- extend the expiration date for FDCCI from 2018 to 2020.[27]

In addition, Congress and the President enacted a law 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 from legacy IT systems, as well as for addressing evolving threats to information security.[28] 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 acquire or develop systems.

Further, in February 2018, OMB issued guidance for agencies on implementing the MGT Act.[29] The guidance was intended to provide agencies additional information regarding the Technology Modernization Fund, and the administration and funding of the related IT working capital funds. Specifically, the guidance encouraged agencies to begin submitting initial project proposals for modernization on February 27, 2018. In addition, in accordance with the MGT Act, the guidance provides 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;[30] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.

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

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

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

[30]The National Protection and Program Directorate (NPPD) was the Department of Homeland Security component responsible for addressing physical and cyber infrastructure protection. The recently enacted 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.

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.[31] 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. Toward 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.

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.

[31]T*he 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.

Responsible agency or agencies	FISMA responsibilities
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-19-275T

The Administration Has Undertaken Efforts to Improve, Modernize, and Strengthen the Security of Federal IT

Beyond the implementation of FITARA, FISMA, and related actions, the administration has also initiated other efforts intended to improve federal IT. 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.[32]

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.[33] The President is the chairman of this council,

[32]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.

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

and the Federal CIO and the United States Digital Service Administrator are among the members.[34]

In addition, on May 11, 2017, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[35] 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[36] 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.

As a result, the *Report to the President on Federal IT Modernization* was issued on December 13, 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 and 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 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 lays out a long-term vision for modernizing the federal government.[37] The agenda identifies 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.

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

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

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

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

The Administration also established 14 related Cross-Agency Priority goals, many of which have elements that involve IT.[38] In particular, the Cross-Agency Priority goal on IT modernization states that modern IT must function as the backbone of how government serves the public in the digital age. This goal establishes 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.

More recently, on May 15, 2018, the President signed Executive Order 13833, *Enhancing the Effectiveness of Agency Chief Information Officers.* Among other things, this executive order is intended to better position agencies to modernize their IT systems, execute IT programs more efficiently, and reduce cybersecurity risks.[39] The order pertains to 22 of the 24 CFO Act agencies: the Department of Defense and the Nuclear Regulatory Commission are exempt.

For the covered agencies, the executive order strengthens 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 directs 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.

[38]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).

[39]Exec. Order No. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers* (May 15, 2018).

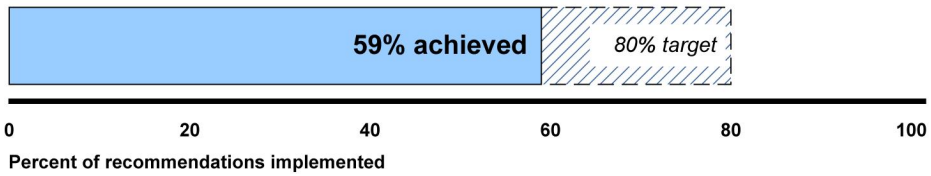
Agencies Have Not Fully Addressed the IT Acquisitions and Operations High-Risk Area

In the February 2017 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.[40] We stressed that OMB and federal agencies should continue to expeditiously implement FITARA and OMB's related guidance, which includes enhancing CIO authority, consolidating data centers, and acquiring and managing software licenses.

Our update to this 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 1,242 recommendations to OMB and federal agencies to address shortcomings in IT acquisitions and operations.

As stated in the update, OMB and agencies should demonstrate government-wide progress in the management of IT investments by, among other things, implementing at least 80 percent of our recommendations related to managing IT acquisitions and operations. As of November 2018, OMB and agencies had fully implemented 732 (or about 59 percent) of the 1,242 recommendations. Figure 1 summarizes the progress that OMB and agencies have 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 November 2018



Source: GAO analysis of Office of Management and Budget and agency data. | GAO-19-275T

[40]GAO-17-317.

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

In all, the various laws, such as FITARA,[41] and related guidance assign 35 IT management responsibilities to CIOs in six key areas. These areas are: leadership and accountability, budgeting, information security, investment management, workforce, and strategic planning.

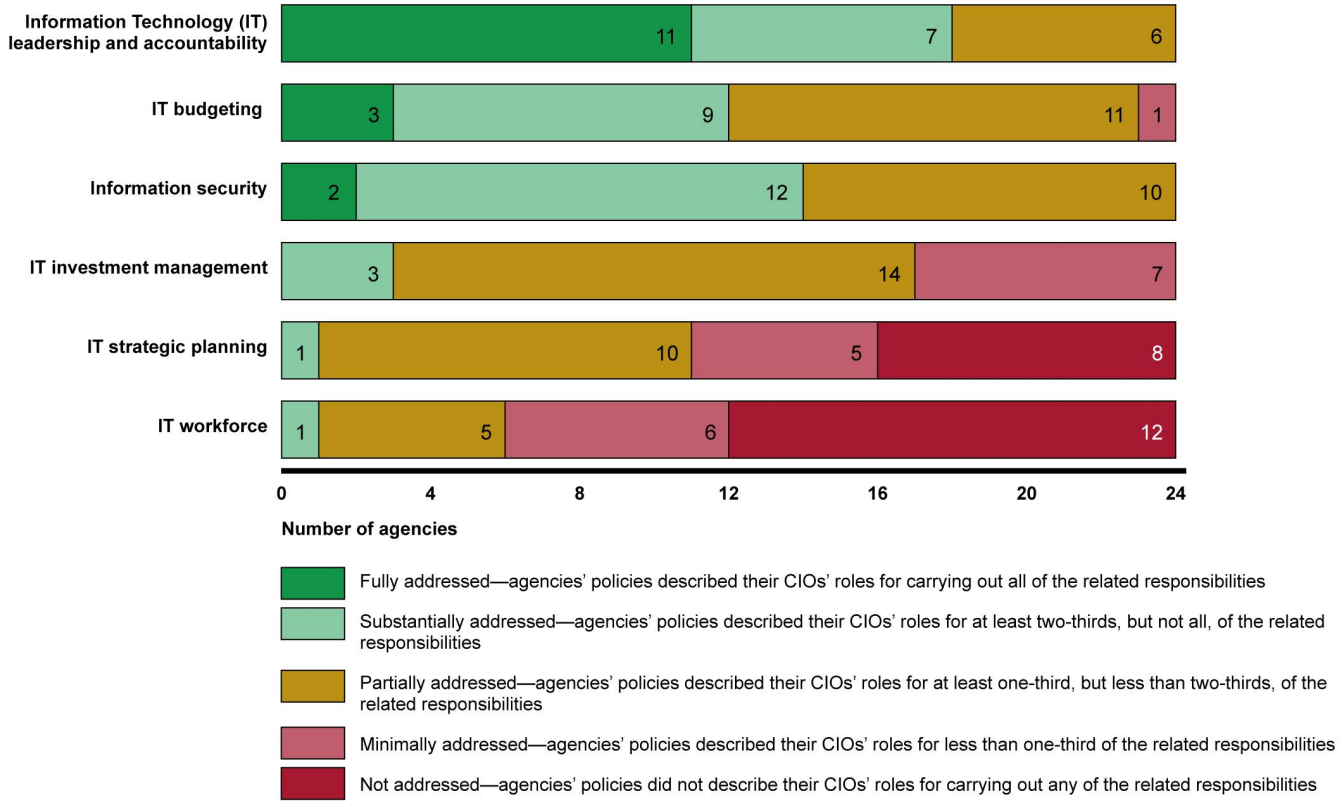
In August 2018, we reported that none of the 24 agencies we reviewed had policies that fully addressed the role of their CIO, as called for by federal laws and guidance.[42] In this regard, a majority of the agencies had fully or substantially addressed the role of their CIOs for the area of leadership 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 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 addressed the role of their CIOs for the six areas.

[41]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).

[42]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).

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



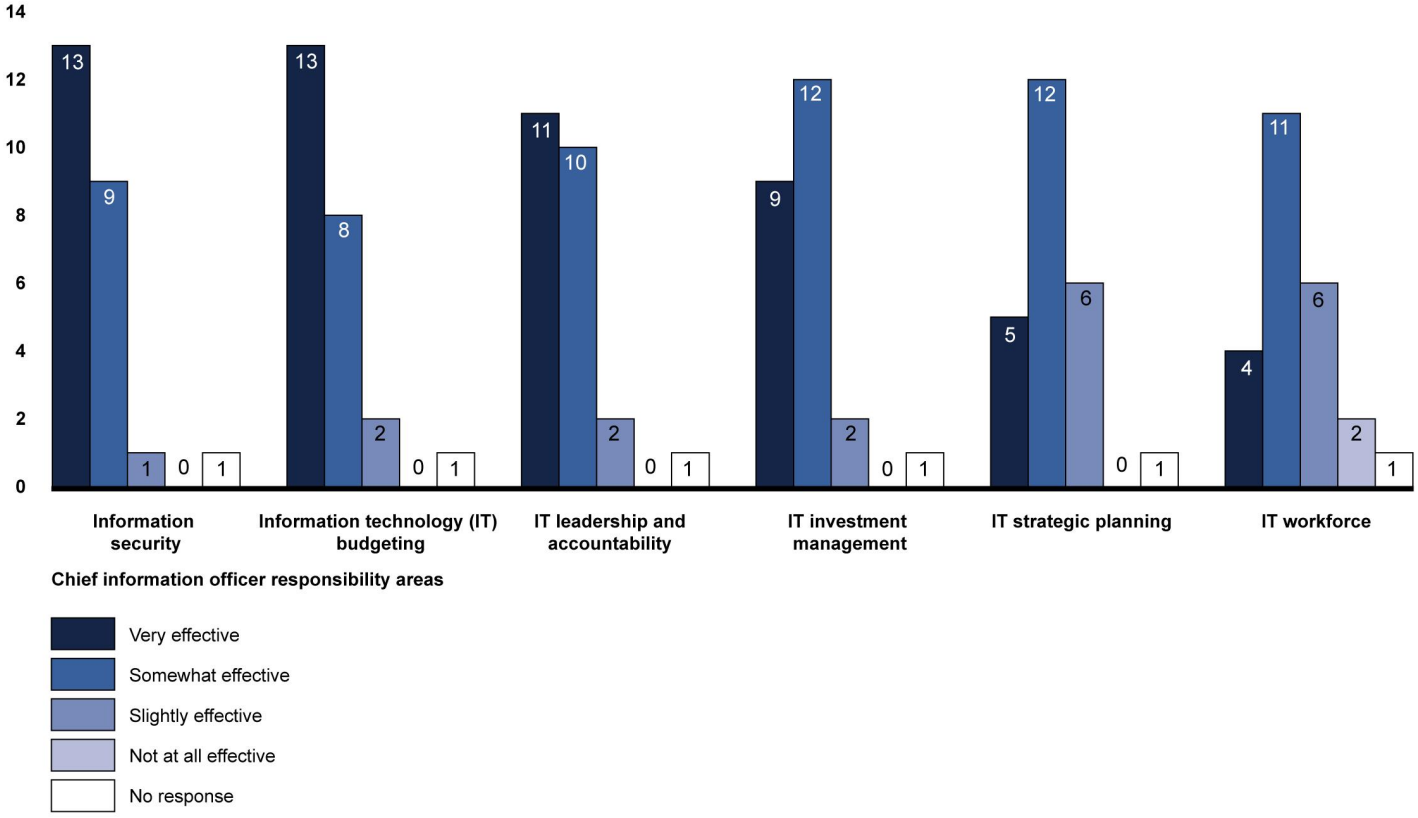
Source: GAO analysis of agency IT management policies. | GAO-19-275T

Despite 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, the CIOs of the 24 selected agencies acknowledged in responses to a survey that we administered 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, agencies 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 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-19-275T

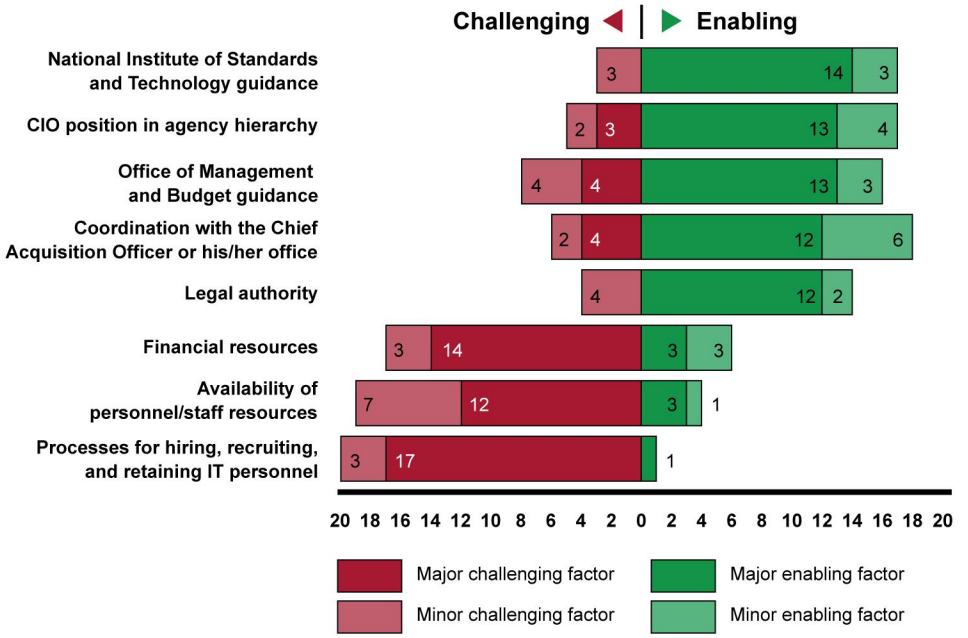
Beyond the actions of the agencies, however, shortcomings in agencies' policies also are partially attributable to two weaknesses in OMB's guidance. First, the guidance does not comprehensively address all CIO responsibilities, such as those related to assessing the extent to which personnel meet IT 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 does not ensure that CIOs have 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 will not be 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 carry out their responsibilities: (1) NIST guidance, (2) the CIO's position in the agency hierarchy, (3) OMB guidance, (4) coordination with the Chief Acquisition Officer (CAO), and (5) legal authority. Further, three factors were cited by CIOs as major factors that have challenged 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-19-275T

Although OMB has issued guidance aimed at addressing the three factors that were identified by at least half of the CIOs as major challenges, the guidance does not fully address those challenges. Further, regarding the financial resources challenge, OMB recently required agencies to provide data on CIO authority over IT spending; however, its guidance does not provide a complete definition of the authority. In the absence of such guidance, agencies have 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 selected 24 federal agencies to improve the effectiveness of CIOs' implementation of their responsibilities for each of the six IT management areas. Most agencies agreed with or had no comments on the recommendations. As of November 2018, all 27 of the recommendations

had not 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.[43] Specifically, according to the guidance:

- CIOs may review and approve IT acquisition strategies and plans, rather than individual IT contracts;[44]
- CIOs can designate other agency officials to act as their representatives, but the CIOs must retain accountability;[45]
- 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 planned acquisition strategies and acquisition plans include IT.

In January 2018, we reported[46] that most of the CIOs at 22 selected agencies[47] were not adequately involved in reviewing billions of dollars of

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

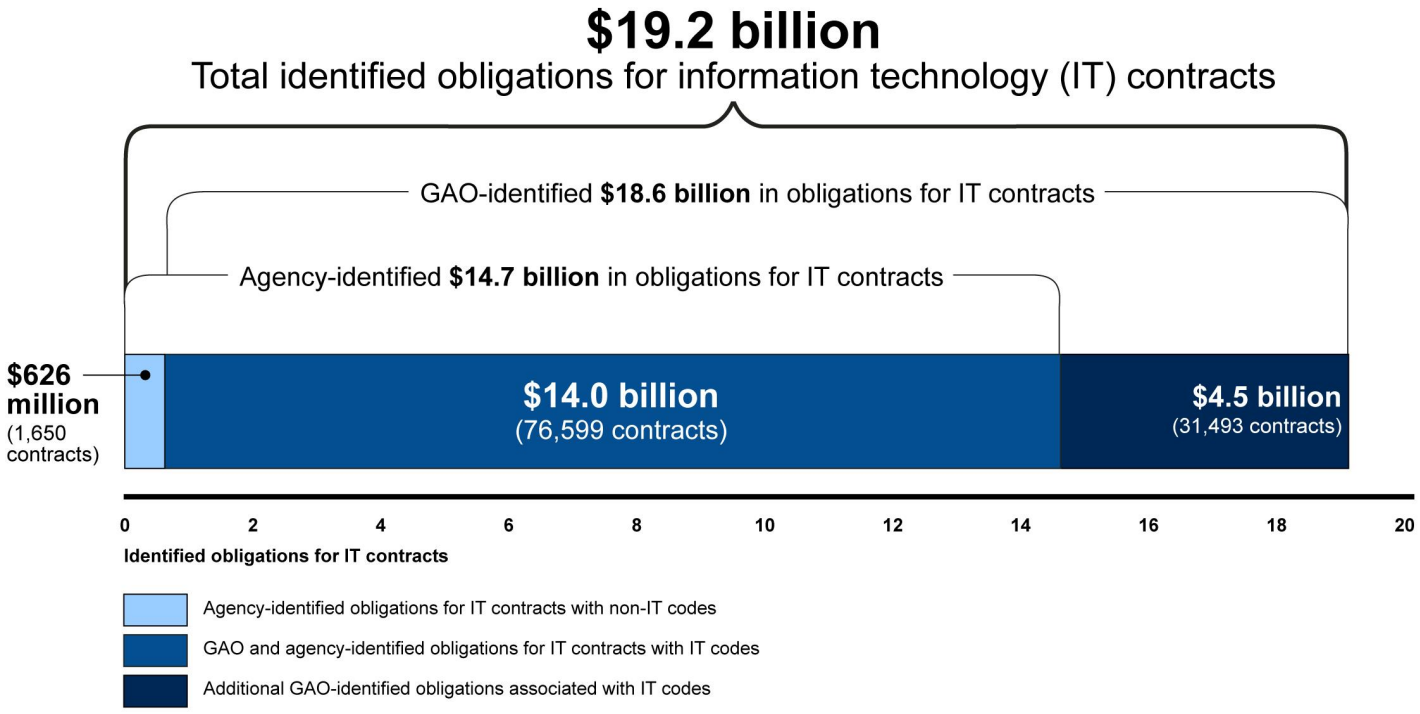
[44]OMB's guidance states that CIOs should only review and approve individual IT contract actions if they are not part of an approved acquisition strategy or plan.

[45]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.

[46]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).

IT acquisitions. 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 contracts with $4.5 billion obligated, raising the total amount obligated to IT contracts by these agencies in fiscal year 2016 to at least $19.2 billion. 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-19-275T

[47]The 22 agencies are 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.

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, 7 agencies did not establish guidance to aid officials in recognizing IT. We concluded that until these agencies involve the acquisitions 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 CIOs cannot effectively provide oversight of these 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 agencies that we evaluated were CIO-reviewed and approved as required by OMB's guidance. The 85 contracts 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 November 2018, 27 of the recommendations had not been implemented.

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

In our February 2017 high-risk update, we stressed that OMB and agencies needed to demonstrate additional progress on achieving data center consolidation savings in order to improve the management of IT acquisitions and operations. Further, 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, in August 2016, OMB issued a memorandum which established the Data Center Optimization Initiative (DCOI) and included guidance on how to implement the data center consolidation and optimization provisions of FITARA.[48] Among other things, the guidance required agencies to consolidate inefficient infrastructure, optimize existing facilities, improve their security posture, and achieve cost savings.

According to agencies, data center consolidation and optimization efforts have resulted in approximately $4.5 billion in cost savings through 2018. However, additional work remains to fully carry out the initiative. Specifically, in a series of reports that we issued from July 2011 through May 2018, 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, data center optimization, and OMB's tracking and reporting on related cost

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

savings.[49] In these reports, we made a total of 160 recommendations to OMB and 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 November 2018, 47 of these 160 recommendations remained unimplemented.

In addition, in a draft report on data center optimization that we have provided to the agencies for comment and plan to issue in early 2019, our preliminary results indicate that agencies continued to report mixed progress toward achieving OMB's goals for closing data centers and realizing the associated savings by September 2018. Specifically, as of August 2018, over half of the agencies reported that they had met, or planned to meet, all of their OMB-assigned closure goals for tiered data centers by the deadline.[50] However, 6 agencies reported that they did not plan to meet their goals for tiered data centers. In addition, as of August 2018, 11 agencies reported that they had already met the goal for closing 60 percent of their non-tiered centers, 3 agencies reported that they planned to meet the goal by the end of fiscal year 2018, and 9 agencies reported that they did not plan to meet the goal by the end of fiscal year 2018.

[49]GAO, *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).

[50]OMB's Memorandum M-16-19 directs agencies to categorize its data centers as a tiered data center, or a non-tiered data center. A tiered data center is defined as one using each of the following: (1) a separate physical space for IT infrastructure; (2) an uninterruptible power supply; (3) a dedicated cooling system or zone; and (4) a backup power generator for a prolonged power outage. All other data centers are to be considered non-tiered data centers.

In all, the 24 agencies reported a total of 6,250 data center closures as of August 2018, which represented about half of the total reported number of federal data centers. In addition, the agencies reported 1,009 planned closures by the end of fiscal year 2018, with an additional 191 closures planned through fiscal year 2023, for a total of 1,200 further closures.

Further, in August 2018, 22 agencies reported that they had achieved $1.94 billion in cost savings for fiscal years 2016 through 2018, while 2 agencies reported that they had not achieved any savings. In addition to that amount, 21 agencies identified a further $0.42 billion in planned savings through fiscal year 2018—for a total of $2.36 billion in planned cost savings from fiscal years 2016 through 2018. Nevertheless, this total is about $0.38 billion less than OMB's goal of $2.74 billion for overall DCOI savings.

Agencies Need to Better Manage Software Licenses to Achieve Savings

In our 2015 high-risk report's discussion of IT acquisitions and operations, we identified the management of software licenses as an area of concern, 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. 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.[51] Of the 24 selected agencies we

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

reviewed, only 2 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 4 had not developed any policies.

Further, we found that only 2 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, 1 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 regularly track and maintain a comprehensive inventory of software licenses and analyze the inventory to identify opportunities to reduce costs and better inform investment decision making.

Most agencies generally agreed with the recommendations or had no comments. As of December 2018, 27 of the 135 recommendations had not been implemented. Table 2 reflects the extent to which the 24 agencies implemented the recommendations in these two areas.

Table 2: Agencies' Implementation of GAO's Software License Management Recommendations, as of December 2018

Agency	Tracks and maintains a comprehensive inventory	Uses inventory to make decisions and reduce costs
Department of Agriculture	Fully	Fully
Department of Commerce	Partially	Fully
Department of Defense	Fully	Fully
Department of Education	Fully	Fully
Department of Energy	Fully	Fully

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

Legend:

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

◐ Partially—the agency had plans to address this recommendation

Source: GAO analysis. | GAO-19-275T

Agencies Need to Address Shortcomings in Information Security Area

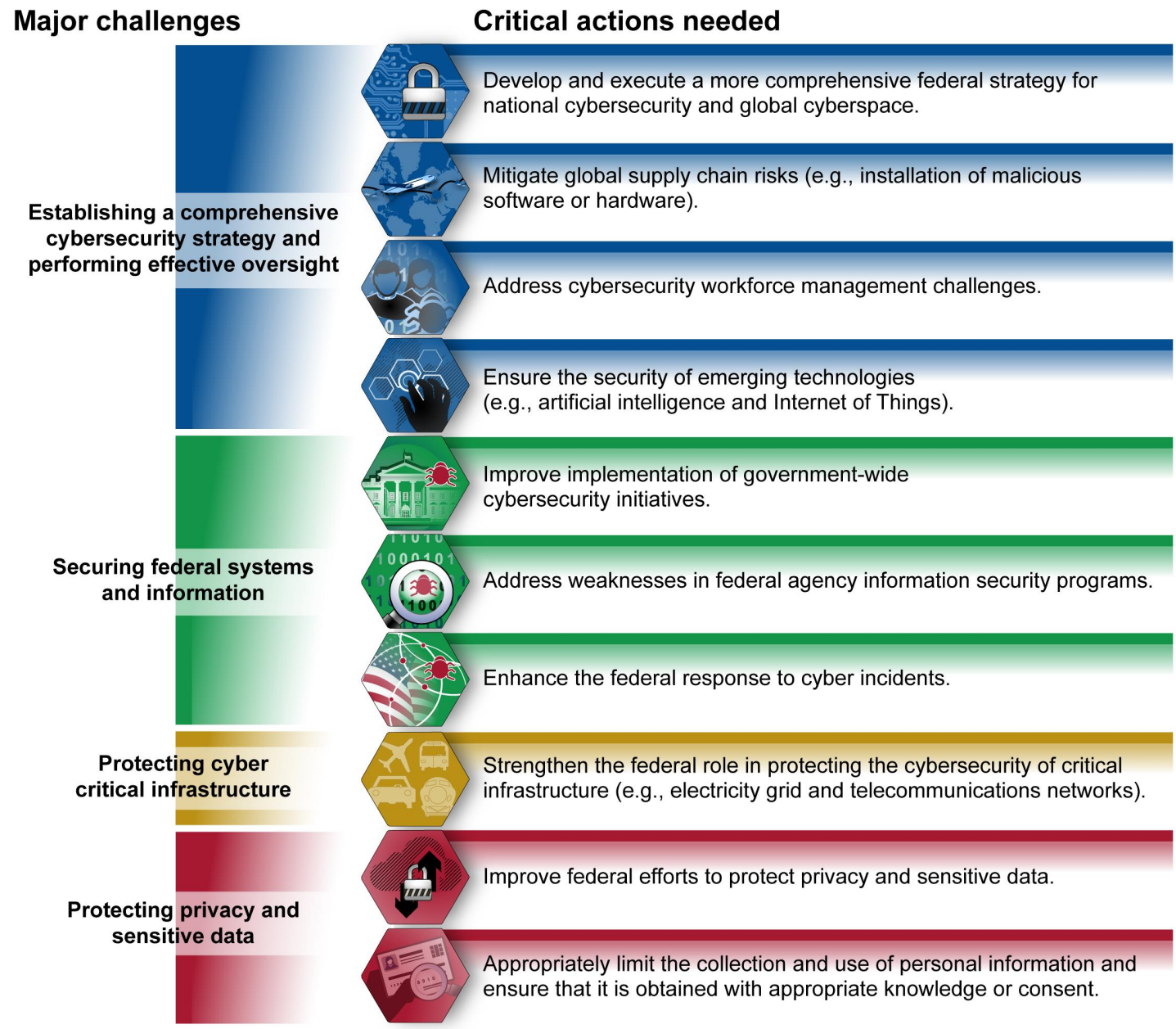
Since information security was added to the high-risk list in 1997, we have consistently identified shortcomings in the federal government's approach to cybersecurity.[52] In particular, in a September 2018 report, we identified four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[53]

To address these challenges, we identified 10 critical actions that the federal government and other entities need to take. For example, in order to address the challenge of securing federal systems and information, we identified 3 actions that the agencies should take: (1) improve implementation of government-wide cybersecurity initiatives, (2) address weaknesses in federal information security programs, and (3) enhance the federal response to cyber incidents. Figure 6 depicts the 10 critical actions to address the four major cybersecurity challenges.

[52]As of the February 2017 update to the high-risk list, this high-risk area is designated as *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information.*

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

Figure 6: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Source: GAO analysis. | GAO-19-275T

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.

Since fiscal year 2010, we have made over 3,000 recommendations to agencies aimed at addressing the 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. Of the roughly 3,000 recommendations made since 2010, 73 percent had been implemented as of November 2018; leaving 688 recommendations unimplemented.

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.[54] 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 strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
- Level 2 Defined: Policies, procedures, and strategy are formalized and documented but not consistently implemented.
- Level 3 Consistently Implemented: Policies, procedures, and strategy 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 strategy are collected across the organizations and used to assess them and make necessary changes.
- Level 5 Optimized: Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

In March 2018, OMB issued its annual FISMA report to Congress, which showed the combined results of the inspectors general's fiscal year 2017 evaluations.[55] Based on data from 76 agency inspector general and independent auditor assessments, OMB determined that the government-wide median maturity model ratings across the five NIST Cybersecurity Framework areas did not exceed a level 3 (consistently implemented). Table 3 shows the inspectors general's median ratings for each of the NIST Cybersecurity Framework areas.

[54]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: Feb. 12, 2014).

[55]Office of Management and Budget. *Federal Information Security Modernization Act of 2014: Annual Report to Congress, Fiscal Year 2017* (Washington, D.C.: March 2018).

Table 3: Median Government-Wide Inspectors General Maturity Model Ratings for Fiscal Year 2017

National Institute of Standards and Technology Cybersecurity Framework area	Median maturity model rating
Identify	Level 3: Consistently implemented
Protect	Level 3: Consistently implemented
Detect	Level 2: Defined
Respond	Level 3: Consistently implemented
Recover	Level 3: Consistently implemented

Source: Office of Management and Budget. | GAO-19-275T

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 the IT modernization 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: manage asset security, protect networks and data, and limit personnel access. 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 2018.

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 2018

Strategies to reduce cybersecurity risks	OMB's target(s)	Civilian agencies' progress in meeting target (average of 23 agencies)	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.	96%	17
Limit Personnel Access	**High Value Asset (HVA) Access Management**: 95 percent of High Value Assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	59%	12
Limit Personnel Access	**Automated Access Management**: 95 percent of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	51%	13
Manage Asset Security	**Hardware Asset Management**: 95 percent of hardware assets covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.	61%	15
Manage Asset Security	**Software Asset Management**: 95 percent of software assets covered by a whitelisting capability.	59%	11
Manage Asset Security	**Authorization Management**: 100 percent of high and moderate impact systems covered by a valid security authorization to operate.	94%	12
Manage Asset Security	**Mobile Device Management**: 95 percent of mobile devices covered by a capability to remotely wipe contents if the device is lost or compromised.	97%	18
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.	4.5 of 6[a]	3[a]
Protect Networks and Data	**Exfiltration and Enhanced Defenses**: At least three of four exfiltration and enhanced defenses metrics have met an implementation target of at least 90 percent.	3.7 of 4	23
Protect Networks and Data	**Data Protection**: At least four of six data protection metrics have met an implementation target of at least 90 percent.	3.4 of 6	12

Source: GAO summary of Office of Management and Budget data. | GAO-19-275T

Note: [a]Many agencies did not meet this goal because not all of their email is analyzed using domain-based message authentication, reporting, and conformance email authentication protocols, as required by Department of Homeland Security's Binding Operational Directive 18-01.

In conclusion, FITARA and FISMA present opportunities for the federal government to address the high-risk areas on improving the management of IT acquisitions and operations and ensuring the security of federal IT, thereby saving billions of dollars. Most agencies have taken steps to execute key IT management and cybersecurity 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. However, 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.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Carol C. Harris, Director, Information Technology, 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), Chris Businsky, Rebecca Eyler, Meredith Raymond, and Jessica Waselkow (Analyst in Charge).

(103115)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548