United States Government Accountability Office

Testimony

Before the Subcommittee on Technology Modernization, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 10:30 a.m. ET
Thursday, July 1, 2021

VETERANS AFFAIRS

Systems Modernization, Cybersecurity, and IT Management Issues Need to Be Addressed

Statement of Carol C. Harris, Director,
Information Technology and Cybersecurity

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

GAO-21-105304

GAO@100 Highlights

Highlights of GAO-21-105304, a testimony before the Subcommittee on Technology Modernization, Committee on Veterans' Affairs, House of Representatives

July 1, 2021

VETERANS AFFAIRS

Systems Modernization, Cybersecurity, and IT Management Issues Need to Be Addressed

Why GAO Did This Study

The use of IT is crucial to helping VA effectively serve the nation's veterans. The department annually spends billions of dollars on its information systems and assets. Its fiscal year 2022 budget request is about $4.8 billion for its Office of Information and Technology and $2.7 billion for electronic health record modernization.

GAO was asked to testify on its prior IT work at VA. Specifically, this testimony summarizes results and recommendations from GAO's issued reports that examined VA's efforts in (1) modernizing VistA and its financial and acquisition management systems; (2) addressing cybersecurity issues; and (3) implementing FITARA. GAO reviewed its recently issued reports that addressed IT and cybersecurity issues at VA and followed up on the department's actions in response to recommendations.

What GAO Recommends

GAO has made numerous recommendations in recent years aimed at improving VA's IT system modernization efforts, cybersecurity program, and implementation of key FITARA provisions. While VA has generally agreed with these, it still needs to implement many of the recommendations.

View GAO-21-105304. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

The Department of Veterans Affairs (VA) has faced long-standing challenges in its efforts to deploy information technology (IT) initiatives in two critical areas needing modernization: the department's aging health information system, known as the Veterans Health Information Systems and Technology Architecture (VistA); and VA's outdated, non-integrated financial and acquisition management systems requiring complex manual work processes that have contributed to the department reporting financial management system functionality as a material weakness. Specifically,

- GAO has reported on the challenges that the department has faced with its three previous unsuccessful attempts to modernize VistA over the past 20 years. In February 2021, GAO reported that VA had made progress toward implementing its fourth effort—a modernized electronic health record system. However, GAO stressed that the department needed to address all critical severity test findings (that could result in system failure) and high severity test findings (that could result in system failure, but have acceptable workarounds) before deploying the system at future locations.
- In March 2021, GAO reported on the department's Financial Management Business Transformation, a program intended to modernize financial and acquisition systems. GAO found that VA had generally adhered to best practices in the areas of program governance, project management, and testing. However, the department had not fully met best practices for developing and managing cost and schedule estimates. GAO recommended that VA follow such practices to help minimize the risks of cost overruns and schedule delays.

GAO has also reported that VA has struggled to secure information systems and associated data; implement information security controls and mitigate known security deficiencies; establish key elements of a cybersecurity risk management program; and identify, assess, and mitigate the risks of information and communications technology supply chains. GAO has made numerous recommendations to VA to address these areas. Many of those recommendations have been addressed, but others have not been fully implemented.

VA has demonstrated mixed results in implementing key provisions of the Federal Information Technology Acquisition Reform Act (commonly referred to as FITARA). Specifically, VA has made substantial progress in improving its licensing of software, which led it to identify $65 million in cost savings. Further, it has made some progress in consolidating its data centers and achieving cost savings and avoidances. However, it has made limited progress in addressing requirements related to managing IT investment risk and enhancing the authority of its Chief Information Officer. Fully implementing the act's provisions would position the department to deliver better service to our veterans through modern, secure technology.

Chairman Mrvan, Ranking Member Rosendale, and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing regarding the Department of Veterans Affairs' (VA) fiscal year 2022 information technology (IT) budget. As you know, the use of IT is crucial to helping VA effectively serve the nation's veterans. The department annually spends billions of dollars on its information systems and assets. Its fiscal year 2022 budget request is about $4.8 billion for the Office of Information and Technology (OI&T), and about $2.7 billion for electronic health record modernization (EHRM).[1]

Over many years, VA has experienced challenges in managing its IT projects and programs, raising questions about the efficiency and effectiveness of OI&T and its ability to deliver intended outcomes needed to help achieve the department's mission. These challenges have spanned a number of critical initiatives related to modernizing the department's existing health information system, the Veterans Health Information Systems and Technology Architecture (VistA); and its current financial and acquisition systems, as part of the Financial Management Business Transformation (FMBT) program. The department has also experienced difficulties in appropriately addressing cybersecurity risks and implementing statutory provisions commonly known as the *Federal Information Technology Acquisition Reform Act* (FITARA).[2]

We have previously reported on these IT management challenges at VA and have made a number of recommendations aimed at improving the department's system acquisitions and operations and cybersecurity

[1]OI&T was formed in 2007 and is responsible for performing key IT functions.

[2]*Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014).

risks.[3] We also designated *VA Health Care* as a high-risk area for the federal government and noted that IT challenges were among the five areas of concern.[4]

At your request, my testimony today summarizes results and recommendations from our issued reports that examined VA's efforts in (1) modernizing VistA and its financial and acquisition management systems; (2) addressing cybersecurity issues; and (3) implementing FITARA.

In developing this testimony, we reviewed our previously issued reports on VA's efforts to modernize its electronic health record and financial and acquisition management systems, address cybersecurity weaknesses, and implement FITARA provisions. We also reviewed our biennial high-risk series which, since 2015, has focused attention on IT challenges related to VA health care. Further, we followed up on the department's

[3]GAO, *Electronic Health Records: VA and DOD Need to Support Cost and Schedule Claims, Develop Interoperability Plans, and Improve Collaboration*, GAO-14-302 (Washington, D.C.: Feb. 27, 2014); *IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments,* GAO-16-494 (Washington, D.C.: June 2, 2016); *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017); *Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations*, GAO-18-264 (Washington, D.C.: May 23, 2018); *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities,* GAO-18-93 (Washington, D.C.: Aug. 2, 2018); *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016); *Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions*, GAO-19-105 (Washington, D.C.: Dec. 18, 2018); *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019); *Electronic Health Records: VA Has Made Progress in Preparing for New System, but Subsequent Test Findings Will Need to Be Addressed,* GAO-21-224 (Washington, D.C.: Feb.11, 2021); and *Veterans Affairs: Ongoing Financial Management System Modernization Program Would Benefit from Improved Cost and Schedule Estimating,* GAO-21-227 (Washington, D.C.: Mar. 24, 2021).

[4]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. VA's issues were highlighted in our 2015 High-Risk Report, GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015), 2017 update, 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), 2019 update, GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019), and 2021 update, GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

actions in response to recommendations we made in our previous reports. The reports cited throughout this statement include detailed information on their scope and methodology.

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

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive benefits, social support, medical care, and lasting memorials. In carrying out this mission, the department operates one of the largest health care delivery systems in America, providing health care to millions of veterans and their families at more than 1,500 facilities.

The department's three major components—the Veterans Benefits Administration (VBA), the Veterans Health Administration (VHA), and the National Cemetery Administration (NCA)—are primarily responsible for carrying out its mission. Specifically, VBA provides a variety of benefits to veterans and their families, including educational opportunities, disability compensation, assistance with home ownership, and life insurance. VHA provides health care services, including primary care and specialty care, and it performs research and development to address veterans' needs. Further, NCA provides burial and memorial benefits to veterans and their families.

VA Relies Extensively on IT

The use of IT is critically important to VA's efforts to provide benefits and services to veterans. As such, the department operates and maintains an IT infrastructure that is intended to provide the backbone necessary to meet the day-to-day operational needs of its medical centers, veteran-facing systems, benefits delivery systems, memorial services, and all other systems supporting the department's mission. The infrastructure is to provide for data storage, transmission, and communications requirements necessary to ensure the delivery of reliable, available, and responsive support to all VA staff offices and administration customers, as well as veterans.

Toward this end, the department operates approximately 240 information systems, manages approximately 314,000 desktop computers and

30,000 laptops, and administers nearly 460,000 network user accounts for employees and contractors to facilitate providing benefits and health care to veterans. These systems are used for the determination of benefits, benefits claims processing, patient admission to hospitals and clinics, and access to health records, among other services.

More specifically, VHA's systems provide capabilities to establish and maintain electronic health records that health care providers and other clinical staff use to view patient information in inpatient, outpatient, and long-term care settings. The department's health information system—VistA—serves an essential role in helping the department to fulfill its health care delivery mission.

VA is in the process of modernizing VistA because it has been in operation for more than 30 years, is costly to maintain, and does not fully support VA's need to electronically exchange health records with other organizations, such as the Department of Defense (DOD). Toward this end, in June 2017, the VA Secretary announced that the department planned to acquire the same Cerner electronic health record system DOD had acquired.[5] VA's effort—the EHRM program—initially deployed the new electronic health record system at the Mann-Grandstaff VA Medical Center in Spokane, Washington, in October 2020, with a phased implementation of the remaining sites planned through 2028. The program has an estimated 10-year life cycle cost of about $16.1 billion.[6]

In addition, since fiscal year 1991 the department has reported on the need for an integrated financial management system and has reported financial management system functionality as a material weakness.[7] This weakness continues to exist because many of VA's systems are outdated, leading to inefficiencies in the reliable, timely, and consistent

[5]In July 2015, DOD awarded a $4.3 billion contract for a commercial electronic health record system developed by Cerner, to be known as MHS GENESIS. The transition to the new system began in February 2017 in the Pacific Northwest region of the United States and is expected to be completed in 2022.

[6]This amount includes $10 billion for the electronic health record contract, $4.3 billion for infrastructure readiness, and $1.8 billion for program management support.

[7]The material weakness in financial management system functionality is linked to VA's outdated legacy financial systems, impacting VA's ability to prepare, process, and analyze financial information that is reliable, timely, and consistent. Legacy system deficiencies necessitate significant manual workarounds and a large number of general ledger adjustments, increasing the risk of processing errors and misstatements in the financial statements.

preparation, processing, and analysis of financial information for the department's consolidated financial statements.

To address this weakness and to improve stewardship and accountability over its resources, VA has for over two decades been pursuing improvements in its business processes and replacement of its existing financial and acquisition management systems with an integrated system. The department's latest improvement efforts are being pursued under the Financial Management Business Transformation (FMBT) program.

VA Requested about $4.8 Billion for OI&T and about $2.7 Billion for EHRM for Fiscal Year 2022

Since 2007, VA has been operating a centralized organization, OI&T, in which most key functions intended for effective management of IT are performed. This office is led by the Assistant Secretary for Information and Technology, also known as VA's Chief Information Officer (CIO).

OI&T is responsible for providing strategy and technical direction, guidance, and policy related to how IT resources are to be acquired and managed for the department. It also is responsible for working with its business partners—such as VHA—to identify and prioritize business needs and requirements for IT systems. Further, OI&T has responsibility for managing the majority of VA's IT-related functions, including the maintenance and modernization of VistA.[8] As of January 2020, OI&T employed over 16,000 government and contractor staff.

According to its budget request for fiscal year 2022, VA is requesting about $4.8 billion for OI&T, which includes $3.1 billion for operations and maintenance, $1.4 billion for personnel and administrative support, and $297 million for new development. Included in the OI&T budget request are several key areas:

- $478 million for infrastructure readiness,
- $361 million for information security,
- $107 million for supply chain modernization, and
- $123 million for the FMBT program.

[8]VistA is a joint program with OI&T and VHA.

Separate from the requested funding for OI&T, VA's budget request included additional funding of approximately $2.7 billion for the EHRM program. This amount included:

- $1.4 billion for the electronic health record contract,
- $952 million for infrastructure support, and
- $286 million for program management.

Federal Laws and Policies Are Intended to Assist with Cybersecurity Challenges

Federal agencies, including VA, and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security, prosperity, and well-being. Because many of these systems contain vast amounts of personally identifiable information, agencies must protect the confidentiality, integrity, and availability of this information. In addition, they must effectively respond to data breaches and security incidents when they occur.

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks. Cybersecurity incidents continue to impact federal entities and the information they maintain. According to the Office of Management and Budget's (OMB) 2019 annual Federal Information Security Modernization Act (FISMA) report to Congress, agencies reported 28,581 information security incidents to the Department of Homeland Security's U.S. Computer Emergency Readiness Team in fiscal year 2019.[9]

[9]Within the Department of Homeland Security, the U.S. Computer Emergency Readiness Team serves as the central federal information security incident center specified by FISMA.

The federal approach and strategy for securing information systems are prescribed by federal law and policy. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[10] In addition, the *Federal Cybersecurity Enhancement Act of 2015* requires federal agencies to protect federal networks through the use of federal intrusion prevention and detection capabilities.[11] Further, Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[12] directs agencies to manage cybersecurity risks to the federal enterprise by, among other things, adhering to practices established in the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (cybersecurity framework).[13]

We have designated information security as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protection of critical cyber infrastructure and, in 2015, to include protecting the privacy of personally identifiable information.[14]

FITARA Is Intended to Help Agencies, Including VA, Improve Their IT Acquisitions

Congress enacted FITARA in December 2014 to improve agencies' acquisitions of IT and enable Congress to better monitor agencies' progress and hold them accountable for reducing duplication and

[10]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 report, 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.

[11]Pub. L. No. 114-113, Division N, Title 2, Subtitle B, 129 Stat. 2963 (2015).

[12]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017), 82 Fed. Reg. 22391 (May 16, 2017).

[13]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018). Available at: Nist.gov/cyberframework.

[14]GAO-19-157SP.

achieving cost savings. The law applies to VA and other covered agencies.[15]

FITARA includes specific requirements related to seven areas, including agency CIO authority, data center consolidation and optimization, risk management of IT investments, and government-wide software purchasing.[16]

- **Agency CIO authority enhancements.** CIOs at covered agencies are required to (1) approve the IT budget requests of their respective agencies, (2) certify that investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB, (3) review and approve contracts for IT, and (4) approve the appointment of other agency employees with the title of CIO.
- **Federal data center consolidation initiative.** Agencies are required to provide OMB with a data center inventory, a strategy for consolidating and optimizing their data centers (to include planned cost savings), and quarterly updates on progress made. The law also requires OMB to develop a goal for how much is to be saved through this initiative, and provide annual reports on cost savings achieved.[17]

[15]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.

[16]FITARA also includes requirements for covered agencies to enhance the transparency and improve risk management of IT investments, annually review IT investment portfolios, expand training and use of IT acquisition cadres, and compare their purchases of services and supplies to what is offered under the federal strategic sourcing initiative that the General Services Administration is to develop. 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.

[17]Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438 (Dec. 19, 2014). The original sunset date for the data center provisions of FITARA has been extended to October 1, 2022. 44 U.S.C. 3601 note.

- **Enhanced transparency and improved risk management in IT investments.** OMB and covered agencies are to make detailed information on federal IT investments publicly available, and department-level CIOs are to categorize their major investments by risk.[18] Additionally, in the case of major investments rated as high risk for four consecutive quarters,[19] the act requires the department-level CIO and the investment's program manager to conduct a review aimed at identifying and addressing the causes of the risk.
- **Government-wide software purchasing program.** The General Services Administration is to enhance government-wide acquisition and management of software and allow for the purchase of a software license agreement that is available for use by all executive branch agencies as a single user. Additionally, *the Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016,* or the "MEGABYTE Act," further enhanced 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.[20]

In June 2015, OMB released guidance describing how agencies are to implement FITARA.[21] This guidance is intended to, among other things:

- assist agencies in aligning their IT resources with statutory requirements;
- establish government-wide IT management controls that will meet the law's requirements, while providing agencies with flexibility to adapt to unique agency processes and requirements;
- clarify the CIO's role and strengthen the relationship between agency CIOs and bureau CIOs; and

[18]"Major IT investment" means a system or an acquisition requiring special management attention because it has significant importance to the mission or function of the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; an unusual funding mechanism; or is defined as major by the agency's capital planning and investment control process.

[19]The IT Dashboard lists the CIO-reported risk level of all major IT investments at federal agencies on a quarterly basis.

[20]Pub. L. No. 114-210 130 Stat. 824 (July 29, 2016).

[21]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.

VA's Management of IT Has Contributed to High-Risk Designations

In 2015, we designated *VA Health Care* as a high-risk area for the federal government and noted that IT challenges were among the five areas of concern.[22] In part, we identified limitations in the capacity of VA's existing systems, including the outdated, inefficient nature of certain systems and a lack of system interoperability—that is, the ability to exchange and use electronic health information—as contributors to the department's IT challenges related to health care.

Also, in February 2015, we added *Improving the Management of IT Acquisitions and Operations* to our list of high-risk areas.[23] Specifically, federal IT investments were too frequently failing or incurring cost overruns and schedule slippages while contributing little to mission-related outcomes. We have previously reported that the federal government has spent billions of dollars on failed IT investments, including at VA.[24]

Our 2017 update to the high-risk report noted that VA had partially met our leadership commitment criterion by involving top leadership in addressing the IT challenges portion of the *VA Health Care* high-risk area;[25] however, it had not met the action plan, monitoring, demonstrated progress, or capacity criteria.[26]

Our March 2019 update to the high-risk series noted that the ratings for the leadership commitment criterion regressed, while the action plan criterion improved for the IT challenges portion of the VA Health Care

[22]GAO-15-290.

[23]GAO-15-290.

[24]GAO, *Information Technology: Management Improvements Are Essential to VA's Second Effort to Replace Its Outpatient Scheduling System*, GAO-10-579 (Washington, D.C.: May 27, 2010); and *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).

[25]GAO-17-317.

[26]GAO uses five criteria to assess progress in addressing high-risk areas: (1) leadership commitment, (2) agency capacity, (3) an action plan, (4) monitoring efforts, and (5) demonstrated progress.

area.[27] The capacity, monitoring, and demonstrated progress criteria remained unchanged. More recently, our March 2021 update noted that the ratings for the capacity criterion improved, but the leadership commitment, action plan, monitoring, and demonstrated progress criteria remained unchanged.[28]

VA Has Historically Faced Challenges in Its Efforts to Modernize IT Systems

VA has faced longstanding challenges in its efforts to modernize two critical IT system: VistA and its financial and acquisition management systems. Specifically, after three unsuccessful attempts to modernize VistA, the department is now undertaking a fourth effort. Similarly, VA is on its third attempt to replace its aging financial and acquisition management systems with an integrated system after previous efforts to replace the systems were unsuccessful and cost hundreds of millions of dollars.

VA's Fourth Effort to Modernize VistA Was Initially Deployed, but Department Needs to Address Unresolved Test Findings Prior to Future Deployments

VA has pursued four efforts over two decades to modernize VistA.[29] These efforts—HealtheVet, the integrated Electronic Health Record (iEHR), VistA Evolution, and EHRM—reflect varying approaches that the department has considered to achieve a modernized health care system. These unsuccessful efforts also reflect the department's lack of success in developing and acquiring a new system as a result of ineffective planning, management, and governance.

HealtheVet

VA undertook its first VistA modernization project, the HealtheVet initiative, in 2001, with the goals of standardizing the department's health care system and eliminating the approximately 130 different versions used by its field locations at that time. HealtheVet was scheduled to be fully implemented by 2018 at a total estimated development and deployment cost of about $11 billion. As part of the initiative, the department had planned to develop or enhance specific areas of system functionality through six projects, which were to be completed between 2006 and 2012.

[27]GAO-19-157SP.

[28]GAO-21-119SP.

[29]GAO, *VA Health IT Modernization: Historical Perspective on Prior Contracts and Update on Plans for New Initiative*, GAO-18-208 (Washington, D.C.: Jan. 18, 2018).

In June 2008, we reported that the department had made progress on the HealtheVet initiative, but noted concerns with its project planning and governance.[30] In June 2009, the VA Secretary announced that the department would stop financing failed projects and improve the management of its IT development projects. Subsequently, in August 2010, the department reported that it had terminated the HealtheVet initiative.

iEHR

VA began its second VistA modernization initiative, the iEHR program, in conjunction with DOD in February 2011. The program was intended to replace the two separate electronic health record systems used by the two departments with a single, shared system. In addition, because both departments would be using the same system, VA and DOD anticipated that this approach would largely sidestep the challenges that had been encountered in trying to achieve interoperability between their two separate systems.

Initial plans called for the development of a single, joint iEHR system consisting of 54 clinical capabilities to be delivered in six increments between 2014 and 2017. Among the agreed-upon capabilities to be delivered were those supporting laboratory, anatomic pathology, pharmacy, and immunizations. According to VA and DOD, the single system was projected to have an estimated life cycle cost of $29 billion through the end of fiscal year 2029.

However, in February 2013, the Secretaries of VA and DOD announced that they would not continue with their joint development of a single electronic health record system. This decision resulted from an assessment of the iEHR program that the secretaries had requested in December 2012 because of their concerns about the program facing challenges in meeting deadlines, costing too much, and taking too long to deliver capabilities. In 2013, the departments abandoned their plan to develop the integrated system and stated that they would again pursue separate modernization efforts.

[30]GAO-08-805.

VistA Evolution

VA initiated its VistA Evolution program as a joint effort of VHA and OI&T in December 2013. The program was to be comprised of a collection of projects and efforts focused on improving the efficiency and quality of veterans' health care, modernizing the department's health information systems, increasing the department's data exchange and interoperability with DOD and private-sector health care partners, and reducing the time it takes to deploy new health information management capabilities. Further, the program was intended to result in lower costs for system upgrades, maintenance, and sustainment. However, VA ended the VistA Evolution program in December 2018 to focus on its new electronic health record system acquisition.

EHRM

In June 2017, VA's Secretary announced a significant shift in the department's approach to modernizing VistA. Specifically, rather than continue to use VistA, the Secretary stated that the department would acquire the same electronic health record system that DOD was implementing. In this regard, DOD awarded a contract to acquire a new integrated electronic health record system developed by the Cerner Corporation. According to the Secretary, VA decided to acquire this same product because it would allow all of VA's and DOD's patient data to reside in one system, thus enabling seamless care between the department and DOD without the manual and electronic exchange and reconciliation of data between two separate systems.

According to the Secretary, this fourth VistA modernization initiative is intended to minimize customization and system differences that currently exist within the department's medical facilities, and ensure the consistency of processes and practices within VA and DOD. When fully operational, the system is intended to be a single source for patients to access their medical history and for clinicians to use that history in real time at any VA or DOD medical facility, which may result in improved health care outcomes. According to VA's Chief Technology Officer, Cerner is expected to provide integration, configuration, testing, deployment, hosting, organizational change management, training, sustainment, and licenses necessary to deploy the system in a manner that meets the department's needs.

In June 2017, the Secretary signed a "Determination and Findings," for a public interest exception[31] to the requirement for full and open competition, and authorized VA to issue a solicitation directly to Cerner. Accordingly, the department awarded a contract to Cerner in May 2018 for a maximum of $10 billion over 10 years.

Cerner is to replace VistA with a commercial electronic health record system. This new system is to support a broad range of health care functions that include, for example, acute care, clinical decision support, dental care, and emergency medicine. When implemented, the new system will be expected to provide access to authoritative clinical data sources and become the authoritative source of clinical data to support improved health, patient safety, and quality of care provided by VA.

Further, in November 2018, the department estimated that an additional $6.1 billion in funding, above the Cerner contract amount, would be needed to fund additional project management support supplied by outside contractors, government labor costs, and infrastructure improvements over a 10-year implementation period.

In August 2020, VA deployed a new scheduling solution—which is a component of its new electronic health record system—at the VA Central Ohio Healthcare System. Deployments of the new electronic health record system are to occur with a phased implementation of the remaining sites over the next decade. Each VA medical facility is expected to continue using VistA until the new system has been deployed at that location.

In October 2020, we reported that VA had made progress toward implementing its new electronic health record system by making system configuration decisions, developing system capabilities and system interfaces, conducting end user training, and completing system testing events.[32] Nevertheless, we noted that the department had not resolved all critical severity test findings (that could result in system failure) and high severity test findings (that could result in system failure, but have acceptable workarounds), as of late September 2020.

We stressed that, if VA did not resolve these test findings prior to initial system deployment, as called for in its testing plan, the department was

[31]Federal Acquisition Regulation, 48 C.F.R. § 6.302-7.

[32]GAO-21-224.

at risk of deploying a system that does not perform as intended and that could negatively impact the likelihood of its successful adoption by users. Accordingly, we recommended that VA delay deployment of the new electronic health record until the test findings were closed or otherwise addressed with workarounds.

In a subsequent report in February 2021, we noted that VA had deployed its new electronic health record system in Spokane, Washington, on October 24, 2020, with no unresolved critical severity test findings and with 306 of the 361 high severity test findings resolved.[33] Of the 55 high severity test findings that remained, 47 had workarounds that were accepted by the user community, seven were associated with future deployments, and one had a solution identified at the time of initial deployment.

VA's actions toward resolving the test findings reflected the implementation of the recommendations that we had made in October 2020. Nevertheless, we pointed out that, as the department moved forward with the deployment of additional capabilities at new locations, it would likely identify new critical and high severity test findings. Further, we stressed that, if the department did not close or appropriately address all critical and high severity test findings prior to deploying at future locations, the system may not perform as intended. Thus, in our February 2021 report, we recommended that VA postpone deployment of its new system at planned locations until any resulting critical and high severity test findings are appropriately addressed. VA concurred with the recommendation and described actions the department planned to take in response.

In March 2021, the VA Secretary announced that the EHRM program would undergo a strategic review after an initial assessment of the program during the Secretary's first month in office. This review was to consist of a full assessment of the program and the assessment period was not planned to exceed 12 weeks. The department noted that the order of subsequent deployments may be revised as a result of this review.

[33]GAO-21-224.

VA's Third Attempt to Modernize Its Financial Management System Would Benefit from Improved Cost and Schedule Estimating

VA's core financial system is approximately 30 years old and is not integrated with other relevant IT systems, which results in inefficient operations and requires complex manual workarounds and reconciliations to meet the department's needs. The department has pursued three efforts to modernize its financial and acquisition systems. These efforts—Core Financial and Logistics System (CoreFLS), Financial and Logistics Integrated Technology Enterprise (FLITE), and Integrated Financial and Acquisition Management System (iFAMS)—reflect varying approaches that the department has considered to achieve modernized financial and acquisition systems. They also reflect the department's weaknesses that were identified in project management and cost and schedule estimating.

CoreFLS

The department's first attempt to replace its financial and asset management systems, CoreFLS, began in 1998. VA had planned to complete CoreFLS in March 2006; however, it terminated development of the system in July 2004 after CoreFLS pilot tests determined that the system did not fully support the department's operations and that the initiative suffered from significant project management weaknesses. According to VA's Office of Inspector General (OIG), the department had obligated about $249 million of the $472 million that had been budgeted for the initiative by the time of its termination.[34]

FLITE

VA began the FLITE initiative in 2005 to develop an integrated financial management and information system. FLITE was to be a multiyear development effort that was projected to deliver a fully operational system by 2014, at a total estimated cost of $608.7 million. However, VA's IG and we issued various reports highlighting challenges the department faced in managing FLITE.[35] The department subsequently terminated the initiative in July 2010 in response to OMB guidance that directed all Chief Financial Officer Act agencies to immediately halt the issuance of new

[34]VA OIG, *Issues at VA Medical Center Bay Pines, Florida and Procurement and Deployment of the Core Financial and Logistics System (CoreFLS)*, 04-01371-177 (Washington, D.C.: Aug. 11, 2004).

[35]GAO-10-40 and VA OIG, *Audit of the FLITE Strategic Asset Management Pilot Project*, 09-03861-238 (Washington, D.C.: Sept. 14, 2010).

procurements for financial system projects until OMB approves new project plans.[36]

FMBT

In March 2021, we reported on VA's third attempt to replace its financial and acquisition systems as part of the FMBT program. We reported that the program had begun implementing the first deployment of certain capabilities of iFAMS at the NCA on November 9, 2020.[37] Full implementation of iFAMS across all of VA is not expected until 2027, at an estimated 10-year life cycle cost of $2.98 billion.

We stressed in our report that following IT management best practices on major transformation efforts, such as the FMBT program, can help build a foundation for ensuring responsibility, accountability, and transparency. In implementing iFAMS, VA had generally met such practices for program governance, Agile project management, and testing and defect management.

However, the department had not fully met certain best practices for developing and managing cost and schedule estimates for iFAMS. Specifically, VA's estimates substantially met one, and partially or minimally met three of the four characteristics associated with reliable cost and schedule estimates, respectively. For example, VA minimally met the "credible" characteristic associated with reliable cost estimates, in part, because it did not compare its cost estimate to an independently developed estimate. As a result, its estimates were not reliable.

Reliable cost and schedule estimates provide a road map for project execution and are critical elements to delivering large-scale IT systems. Without reliable estimates, VA management may not have the information necessary for informed decision-making. Further, following cost and schedule best practices helps minimize the risk of cost overruns and schedule delays and would better position the FMBT program for effective and successful implementation on future deployments.

[36]Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: Immediate Review of Financial Systems IT Projects*, OMB Memorandum M-10-26 (June 28, 2010).

[37]GAO-21-227.

Accordingly, we made recommendations for the FMBT program to develop reliable cost and schedule estimates to help ensure that the FMBT program is consistent with best practices for estimating. VA concurred with the recommendations and described actions the department intends to take.

VA Faces Key Security Challenges as It Modernizes and Secures Its Information Systems

In several reports issued since fiscal year 2016, we have highlighted key challenges that VA has faced in safeguarding its information and information systems. These relate to the department effectively implementing the federal approach and strategy for securing information systems, information security controls, and mitigating known security deficiencies; and establishing elements of its cybersecurity risk management program. Our work has stressed the need for VA to address these challenges, as well as manage IT supply chain risks, as it modernizes and secures its information systems.

Effectiveness in Implementing the Federal Approach and Strategy for Securing Information Systems

The federal approach and strategy for securing information systems are prescribed by federal law and policy, including FISMA and the executive order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[38] Accordingly, federal reports describing agency implementation of this law and policy, and reports of related agency information security activities, indicate the effectiveness of agencies' efforts to implement the federal approach and strategy.

In December 2018, we reported on the effectiveness of the government's approach and strategy for securing its systems.[39] We noted that the 23 civilian agencies covered by the Chief Financial Officers Act of 1990 have often not effectively implemented the federal government's approach and

[38]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017), 82 Fed. Reg. 22391 (May 16, 2017).

[39]GAO-19-105.

strategy for securing information systems, including VA.[40] Our report pointed out that VA was deficient or had material weaknesses in four indicators of its effectiveness in implementing the federal approach and strategy for securing information systems.[41]

Effectively Implementing Information Security Controls and Mitigating Known Security Deficiencies

FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The law is also intended to ensure the effective oversight of information security risks, including those throughout civilian, national security, and law enforcement agencies.

VA has had difficulties in effectively implementing security controls over its information and information systems. Specifically, we identified control deficiencies during an examination of the department's high-impact systems[42] that we reported on in 2016.[43] In those reports, we described deficiencies in VA's implementation of access controls, patch management, and contingency planning. The deficiencies existed, in part,

[40]The 23 civilian Chief Financial Officers Act of 1990 agencies are 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. We did not include the Department of Defense in the scope of our audit because the Federal Cybersecurity Enhancement Act of 2015 only applies to civilian agencies.

[41]The four areas of effectiveness in implementing the federal approach and strategy for securing information systems are the Inspector General Information Security Program Ratings; the Inspector General Internal Control Deficiencies over Financial Reporting; CIO Cybersecurity Cross-Agency Priority Goal Targets; and the OMB Management Assessment Ratings.

[42]High-impact systems are those systems where the loss of confidentiality, integrity, or availability of the systems or the information they contain can have a severe or catastrophic adverse effect on an organization's operations, assets, or individuals. Such an impact can result in loss or degradation of mission capability, severe harm to individuals, or major financial loss.

[43]GAO-16-501 and GAO-16-691SU.

because the department had not effectively implemented key elements of its information security program.

We recommended 74 actions for the department to take to improve its cybersecurity program and remedy known control deficiencies with selected high-impact systems.[44] As of June 2021, VA had implemented 70 (or about 95 percent) of the 74 recommendations, which included all of the recommendations to improve the department's information security program. However, the four remaining recommendations relate to weaknesses in access controls and configuration management. Until VA addresses these remaining shortcomings, it will continue to have limited assurance that its sensitive information and information systems are sufficiently safeguarded.

Fully Establishing Elements of a Cybersecurity Risk Management Program

VA has not effectively managed its cybersecurity risks. In July 2019, we reported that the department had fully met only one of the five foundational practices for establishing a cybersecurity risk management program.[45] Although VA established the role of a cybersecurity risk executive, the department had not fully:

- developed a cybersecurity risk management strategy that addressed key elements, such as risk tolerance and risk mitigation strategies;
- documented risk-based policies that required the department to perform agency-wide risk assessments;
- conducted an agency-wide cybersecurity risk assessment to identify, assess, and manage potential enterprise risks; or
- established coordination between cybersecurity and enterprise risk management.

VA concurred with our four recommendations to address these deficiencies and described efforts under way to institutionalize

[44]We issued five recommendations in the publicly available report and an additional 69 recommendations in a separate report with limited distribution that we provided directly to VA. The accompanying report included recommendations to address weaknesses identified related to access control, patch management, and contingency planning. (GAO-16-501 and GAO-16-691SU, respectively).

[45]GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address* Challenges, GAO-19-384 (Washington, D.C.: Jul. 25, 2019).

coordination between cybersecurity and enterprise risk management functions. However, as of June 2021, these recommendations remain open. Until the department fully establishes a cybersecurity risk management program, its ability to convey acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance will be diminished.

Managing IT Supply Chain Risks as Part of IT Modernization Programs

Assessing and managing supply chain risks are important considerations for agencies, including VA, when operating and modernizing IT systems. Supply chain risk management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology (ICT) product and service supply chains. Many of the manufacturing inputs for these ICT products and services originate from a variety of sources throughout the world. The foundational practices comprising ICT SCRM are:

- establishing executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
- developing an agency-wide ICT SCRM strategy for providing the organizational context in which risk-based decisions will be made;
- establishing an approach to identify and document agency ICT supply chain(s);
- establishing a process to conduct agency-wide assessments of ICT supply chain risks that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization;
- establishing a process to conduct a SCRM review of a potential supplier that may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services;
- developing organizational ICT SCRM requirements for suppliers to ensure that suppliers are adequately addressing risks associated with ICT products and services; and
- developing organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

As we reported in December 2020,[46] few of the 23 civilian Chief Financial Officers Act agencies, which includes VA, had implemented the seven selected foundational practices for managing ICT supply chain risks. None of the 23 agencies we reviewed had fully implemented all of the SCRM practices and 14 of the 23 agencies had not implemented any of the practices. The practice with the highest rate of implementation was implemented by only six agencies. Moreover, one practice had not been implemented by any of the agencies.

We made a total of 145 recommendations to the 23 agencies to fully implement foundational practices in their organization-wide approaches to ICT SCRM.[47] Until the agencies implement all of the foundational ICT SCRM practices, they will be limited in their ability to address supply chain risks across their organizations effectively.

VA Has Demonstrated Mixed Results toward Implementing Key FITARA Provisions

FITARA includes provisions for covered federal agencies to, among other things, enhance government-wide acquisition and management of software, improve the risk management of IT investments, consolidate data centers, and enhance CIOs' authorities. Since its enactment, we have reported numerous times on VA's efforts toward implementing FITARA.[48]

VA has demonstrated mixed results in implementing key FITARA provisions. Specifically, VA has made substantial progress toward improving its licensing of software. In addition, the department has made some progress in consolidating its data centers and achieving cost savings and avoidances. However, the department has made limited progress in addressing requirements related to IT investment risk and CIO authority enhancement.

Software Licensing

VA has addressed our recommendations regarding federal software licensing requirements. In May 2014, we reported on federal agencies'

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

[47]We made the 145 recommendations in a separate report with limited distribution GAO-21-164SU.

[48]GAO-16-494, GAO-16-469, GAO-18-148, GAO-18-264, and GAO-18-93.

management of software licenses and stressed that better management was needed to achieve significant savings government-wide.[49]

Specifically, regarding VA, we noted that the department did not have comprehensive policies that included the establishment of clear roles and central oversight authority for managing enterprise software license agreements, among other things. We also noted that it had not established a comprehensive software license inventory, a leading practice that would help the department to adequately manage its software licenses.

The inadequate implementation of these and other leading practices in software license management was partially due to weaknesses in the department's policies related to licensing management. Thus, we made six recommendations to VA to improve its policies and practices for managing licenses. For example, we recommended that the department 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.

Since our 2014 report, VA has taken actions to implement all six recommendations. Among these actions, the department created a solution to generate and maintain a comprehensive inventory of software licenses using automated tools for the majority of agency software license spending and/or enterprise-wide licenses. Additionally, the department implemented a solution to analyze agency-wide software license data, including usage and costs; it subsequently identified approximately $65 million in cost savings over 3 years due to analyzing one of its software licenses.

Data Center Consolidation

VA has made progress in consolidating and optimizing its data centers. Specifically, as of August 2020, the department had addressed our recommendation to meet its data center closure goals and reported that it

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

had closed 13 data centers to meet its fiscal year 2020 goal of closing 12 data centers.[50]

Further, as of December 2020, the department had addressed our recommendation to meet its data center cost savings goals. The department reported that it had achieved $3.38 million in fiscal year 2020 data center-related cost savings and avoidances, which exceeded its goal of $3.1 million.

Also, as of December 2020, VA reported meeting two of OMB's four data center optimization targets related to advanced energy metering and server utilization.[51] However, the department did not meet OMB's two other targets—for virtualization and data center availability.

Risk Management

VA has made limited progress in addressing the FITARA requirements related to managing the risks associated with IT investments. In June 2016, we reported on VA's CIO's ratings of risk assigned to investments.[52] We noted that the department had reviewed compliance with risk management practices, but had not assessed active risks when developing its CIO ratings.

Specifically, when developing CIO ratings, VA chose to focus on investments' risk management processes, such as whether a process was in place or whether a risk log was current. In addition, VA's CIO rating process considered several specific risk management criteria: whether an investment (1) had a risk management strategy, (2) kept the risk register current and complete, (3) clearly prioritized risks, and (4) put mitigation plans in place to address risks.

However, the department's approach did not consider active risks, such as funding cuts or staffing changes, which can detail the probability and impact of pending threats to success. As a result, we recommended that VA factor active risks into its CIO ratings. We also recommended that the

[50]GAO, *Data Center Optimization: Additional Agency Actions Needed to Meet OMB Goals,* GAO-19-241 (Washington, D.C.: Apr. 11, 2019).

[51]OMB's virtualization metric refers to the number of servers and mainframes serving as virtual hosts in agency-managed data centers. Server utilization describes the number of underutilized production servers in federal data centers.

[52]GAO-16-494.

department ensure that these ratings reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals. VA concurred with the recommendations and cited actions it planned to take to address them. As of June 2021, these recommendations had not been implemented.

CIO Authorities

VA has made limited progress in addressing the CIO authority requirements of FITARA. Specifically, in November 2017, we reported on agencies' efforts to utilize incremental development practices for selected major investments.[53] Regarding VA, we noted that the department's CIO had certified the use of adequate incremental development for all 10 of the department's major IT investments.

However, VA had not updated the department's policy and process for the CIO's certification of major IT investments' adequate use of incremental development, in accordance with OMB's guidance on the implementation of FITARA. We recommended that the department do so and an OI&T official reported in June 2021 that the department was in the process of finalizing its guidance related to addressing this recommendation. The guidance was undergoing final review by relevant stakeholders and the official anticipated the guidance would be finalized by the end of June.

Further, in January 2018, we reported on the need for agencies to involve CIOs in reviewing IT acquisition plans and strategies.[54] We noted that VA's CIO did not review IT acquisition plans or strategies and that the Chief Acquisition Officer was not involved in the process of identifying IT acquisitions. Accordingly, we recommended that the VA Secretary ensure that the office of the Chief Acquisition Officer is involved in the process to identify IT acquisitions. We also recommended that the Secretary ensure that the acquisition plans or strategies are reviewed and approved in accordance with OMB guidance.

The department concurred with the recommendations and, in November 2019, issued a Standard Operating Procedure that required the CIO and Chief Acquisition Officer to work together to review and approve all IT acquisition strategies and plans. However, as of May 2021, the

[53]GAO-18-148.

[54]GAO-18-42.

department had not provided evidence that the CIO (or designee) was reviewing and approving selected IT acquisition plans.

In addition, in reporting on federal CIOs in August 2018, we noted that federal laws and guidance assign to agency CIOs 35 key responsibilities for effectively managing IT, which should be documented in agencies' policies. These responsibilities are in six areas: leadership and accountability, strategic planning, workforce, budgeting, investment management, and information security.

We reported that VA had only fully addressed two of the six key CIO management responsibility areas that we identified—IT Leadership and Accountability and Information Security.[55] The department had partially addressed IT Budgeting, minimally addressed IT Investment Management, and had not addressed IT Strategic Planning or IT Workforce. Thus, we recommended that the VA Secretary ensure that the department's IT management policies address the role of the CIO for key responsibilities in the four areas we identified.

The department concurred with the recommendation and acknowledged that many of the responsibilities provided to the CIO were not explicitly formalized by VA policy. However, as of June 2021, the department had not implemented this recommendation.

In conclusion, VA has long struggled to overcome IT management challenges, which have resulted in a lack of system capabilities needed to successfully implement critical initiatives related to modernizing its health information system and financial and acquisition systems. We have made recommendations aimed at helping the department to achieve its goals related to these efforts. However, if the department continues to experience the challenges that we have previously identified and does not take actions to address our recommendations, it may jeopardize its ability to effectively support the EHRM and FMBT programs.

Further, the lack of key cybersecurity management elements at VA is concerning given that agencies' systems are increasingly susceptible to the multitude of cyber-related threats that exist. As VA continues to

[55]Based on our reviews of FITARA and other relevant laws and guidance, we identified 35 key CIO IT management responsibilities and categorized them in six management areas for this report. GAO-18-93.

pursue modernization efforts, it is critical that the department's IT budget supports efforts to adequately secure its systems.

Additionally, the department has been challenged in fully implementing the risk management, data center consolidation, and CIO authorities provisions of FITARA, which has limited its ability to improve its management of IT acquisitions. Until the department fully implements the act's provisions, Congress' ability to effectively monitor VA's progress and hold it fully accountable for reducing duplication and achieving cost savings may be hindered.

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

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Carol C. Harris, Director, Information Technology Management Issues, at (202) 512-4456 or harrisc@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 Mark Bird (Assistant Director), Eric Trout (Analyst in Charge), Justin Booth, Rebecca Eyler, Valerie Hopkins, Jeff Knott, George Kovachick, Michael LaForge, Scott Pettis, Meredith Raymond, Rachael Scott, Gabriel Siewert, Kevin Walsh, Jessica Waselkow, Eric Winter, and Charles Youman.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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, https://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, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

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