United States Government Accountability Office

Testimony

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

For Release on Delivery
10:15 a.m. ET
Tuesday, April 2, 2019

VETERANS AFFAIRS

Addressing IT Management Challenges Is Essential to Effectively Supporting the Department's Mission

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

Chair Lee, Ranking Member Banks, and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing regarding the Department of Veterans Affairs' (VA) Office of Information and Technology (OI&T). As you know, the use of information technology (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—VA's budget for IT now exceeds $4 billion annually.

However, 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 advance the department's mission. These challenges have spanned a number of critical initiatives related to modernizing the department's (1) health information system, the Veterans Health Information Systems and Technology Architecture (VistA); (2) program to support family caregivers; and (3) benefits management system. The department has also experienced challenges in implementing provisions of the *Federal Information Technology Acquisition Reform Act* (commonly referred to as FITARA),[1] and in appropriately addressing cybersecurity risks.

We have previously reported on these IT management challenges at VA and have made recommendations aimed at improving the department's

[1]*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).

system acquisitions and operations.[2] At your request, my testimony today summarizes results and recommendations from our work at the department that examined its system modernization efforts, as well as its efforts toward implementing FITARA and addressing cybersecurity issues.

In developing this testimony, we relied on our recently issued reports that addressed IT management issues at VA and our bi-annual high-risk series.[3] We also incorporated information on the department's actions in response to recommendations we made in our previous reports. The reports cited throughout this statement include detailed information on the scope and methodology of our prior reviews.

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

[2]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); *VA Health Care: Actions Needed to Address Higher-Than-Expected Demand for the Family Caregiver Program*, GAO-14-675 (Washington, D.C.: Sept. 18, 2014); *Veterans Benefits Management System: Ongoing Development and Implementation Can Be Improved; Goals Are Needed to Promote Increased User Satisfaction*, GAO-15-582 (Washington, D.C.: Sept. 1, 2015); *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); and *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019).

[3]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), and 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).

.

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 medical care, benefits, social support, 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 Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA)—are primarily responsible for carrying out its mission. More specifically, VHA provides health care services, including primary care and specialized care, and it performs research and development to address veterans' needs. VBA provides a variety of benefits to veterans and their families, including disability compensation, educational opportunities, assistance with home ownership, and life insurance. 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.

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.

Specifically, VistA is an integrated medical information system that was developed in-house by the department's clinicians and IT personnel, and has been in operation since the early 1980s.[4] The system consists of 104 separate computer applications, including 56 health provider applications; 19 management and financial applications; eight registration, enrollment, and eligibility applications; five health data applications; and three information and education applications. Within VistA, an application called the Computerized Patient Record System enables the department to create and manage an individual electronic health record for each VA patient.

In June 2017, the former VA Secretary announced that the department planned to acquire the same Cerner electronic health record system that the Department of Defense (DOD) has acquired.[5] VA's effort—the Electronic Health Record Modernization (EHRM) program—calls for the deployment of a new electronic health record system at three initial sites in 2020, with a phased implementation of the remaining sites over the next decade.

In addition, VBA relies on the Veterans Benefits Management System (VBMS) to collect and store information such as military service records, medical examinations, and treatment records from VA, DOD, and private medical service providers. In 2014, VA issued its 6-year strategic plan, which emphasizes the department's goal of increasing veterans' access to benefits and services, eliminating the disability claims backlog, and ending veteran homelessness. According to the plan, the department intends to improve access to benefits and services through the use of enhanced technology to provide veterans with access to more effective care management.

[4]VistA began operation in 1983 as the Decentralized Hospital Computer Program. In 1996, the name of the system was changed to VistA.

[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.

The plan also calls for VA to eliminate the disability claims backlog by fully implementing an electronic claims process that is intended to reduce processing time and increase accuracy. Further, the department has an initiative under way that provides services, such as health care, housing assistance, and job training, to end veteran homelessness. Toward this end, VA is working with other agencies, such as the Department of Health and Human Services, to implement more coordinated data entry systems to streamline and facilitate access to appropriate housing and services.

VA Manages IT Resources Centrally

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—VA's Chief Information Officer (CIO). The office 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, and for working closely with its business partners—such as VHA—to identify and prioritize business needs and requirements for IT systems. Among other things, OI&T has responsibility for managing the majority of VA's IT-related functions, including the maintenance and modernization of VistA.[6] As of January 2019, OI&T was comprised of about 15,800 staff, with more than half of these positions filled by contractors.

VA Is Requesting about $5.9 Billion for IT and a New Electronic Health Record System for Fiscal Year 2020

VA's fiscal year 2020 budget request includes about $5.9 billion for OI&T and its new electronic health record system. Of this amount, about $4.3 billion was requested for OI&T, which represents a $240 million increase over the $4.1 billion enacted for 2019. The request seeks the following levels of funding:

- $401 million for new systems development efforts to support current health care systems platforms, and to replace legacy systems, such as the Financial Management System;
- approximately $2.7 billion for the operations and maintenance of existing systems, which includes $327.3 million for infrastructure readiness that is to support the transition to the new electronic health record system; and
- approximately $1.2 billion for administration.

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

Additionally, the department requested about $1.6 billion for the EHRM program. This amount is an increase of $496 million over the $1.1 billion that was enacted for the program for fiscal year 2019. The request includes the following:

- $1.1 billion for the contract with the Cerner Corporation to acquire the new system,
- $161,800 for program management, and
- $334,700 for infrastructure support.

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.[7] 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.[8] 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.[9]

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

[7]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) and 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).

[8]GAO-15-290.

[9]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); *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).

area; however, it had not met the action plan, monitoring, demonstrated progress, or capacity criteria.

We have also identified VA as being among a handful of departments with one or more archaic legacy systems. Specifically, in our May 2016 report on legacy systems used by federal agencies, we identified two of VA's systems as being over 50 years old—the Personnel and Accounting Integrated Data system and the Benefits Delivery Network system.[10] These systems were among the 10 oldest investments and/or systems that were reported by 12 selected agencies.

Accordingly, we recommended that the department identify and plan to modernize or replace its legacy systems. VA addressed the recommendation in May 2018, when it provided a Comprehensive Information Technology Plan that showed a detailed roadmap for the key programs and systems required for modernization. The plan included time frames, activities to be performed, and functions to be replaced or enhanced. The plan also indicated that the Personnel and Accounting Integrated Data system and the Benefits Delivery Network system are to be decommissioned in quarters 3 and 4 of fiscal year 2019, respectively.

Our March 2019 update to our high-risk series noted that the ratings for leadership commitment criterion regressed, while the action plan criterion improved for the IT Challenges portion of the *VA Health Care* area.[11] The capacity, monitoring, and demonstrated progress criteria remained unchanged. Our work continued to indicate that VA was not yet able to demonstrate progress in this area.

Since its 2015 high-risk designation, we have made 14 new recommendations in the *VA Health Care* area, 12 of which were made since our 2017 high-risk report was issued. For example, in June 2017, to address deficiencies we recommended that the department take six actions to provide clinicians and pharmacists with improved tools to support pharmacy services to veterans and reduce risks to patient safety. VA generally concurred with these recommendations; however, all of them remain open.

[10]GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

[11]GAO-19-157SP.

FITARA Is Intended to Help VA and Other Agencies 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 achieving cost savings. The law applies to VA and other covered agencies.[12] It 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.[13]

- **Agency CIO authority enhancements.** CIOs at covered agencies are required to (1) approve the IT budget requests of their respective agencies, (2) certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget (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

[12]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.

[13]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.

requires OMB to develop a goal for how much is to be saved through this initiative, and provide annual reports on cost savings achieved.[14]

- **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 IT investments by risk.[15] Additionally, in the case of major investments rated as high risk for 4 consecutive quarters,[16] the act required that the department-level CIO and the investment's program manager 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.[17]

In June 2015, OMB released guidance describing how agencies are to implement FITARA.[18] This guidance is intended to, among other things:

- assist agencies in aligning their IT resources with statutory requirements;

[14]In November 2017, the *FITARA Enhancement Act of 2017* was enacted into law to extend the sunset date for the data center provisions of FITARA. The law's data center consolidation and optimization provisions currently expire on October 1, 2020. Pub. L. No. 115-88 (Nov. 21, 2017).

[15]"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.

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

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

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

- 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
- strengthen CIO accountability for IT costs, schedules, performance, and security.

VA and Other Agencies Face Cybersecurity Risks

The federal approach and strategy for securing information systems is prescribed by federal law and policy. The Federal Information Security Modernization Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[19] In addition, the *Federal Cybersecurity Enhancement Act of 2015* requires protecting federal networks through the use of federal intrusion prevention and detection capabilities. Further, Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[20] directs agencies to manage cybersecurity risks to the federal enterprise by, among other things, using the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*[21] (cybersecurity framework).

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.

[19]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.

[20]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).

[21]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

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 OMB's 2018 annual FISMA report to Congress, agencies reported 35,277 information security incidents to DHS's U.S. Computer Emergency Readiness Team[22] in fiscal year 2017.

VA Has Made Limited Progress toward Addressing IT System Modernization Challenges

VA has made limited progress toward addressing the IT management challenges for three critical initiatives: VistA, the Family Caregiver Program, and VBMS. Specifically, the department has recently initiated its fourth effort to modernize VistA, but uncertainty remains regarding the program's governance. In addition, although VA has taken steps to address our recommendations for the Family Caregiver Program and VBMS, the department has not fully implemented most of them.

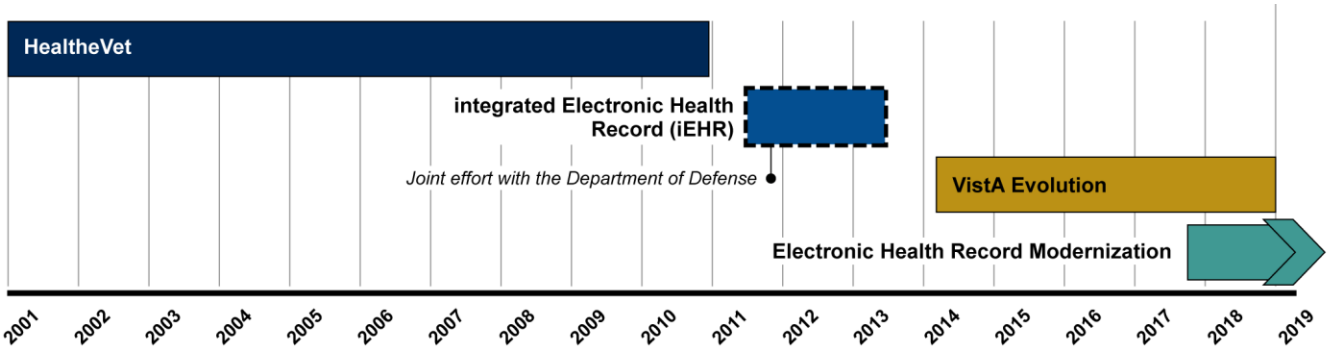
VA Recently Initiated Its Fourth Effort to Modernize VistA

VA has pursued four efforts over nearly 2 decades to modernize VistA.[23] 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. Figure 1 shows a timeline of the four efforts that VA has pursued to modernize VistA since 2001.

[22]Within DHS, the U.S. Computer Emergency Readiness Team is a component of the National Cybersecurity and Communications Integration Center. It serves as the central federal information security incident center specified by FISMA.

[23]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).

Figure 1: Timeline of the Department of Veterans Affairs Four Efforts to Modernize the Veterans Health Information Systems and Technology Architecture (VistA) Since 2001



Source: GAO analysis of Department of Veterans Affairs data. | GAO-19-476T

HealtheVet

In 2001, VA undertook its first VistA modernization project, the HealtheVet initiative, with the goals of standardizing the department's health care system and eliminating the approximately 130 different systems 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 effort, 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.

In June 2008, we reported that the department had made progress on the HealtheVet initiative, but noted concerns with its project planning and governance.[24] In June 2009, the Secretary of Veterans Affairs announced that VA 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

In February 2011, VA began its second VistA modernization initiative, the iEHR program, in conjunction with DOD. 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, this approach was

[24]GAO-08-805.

expected to 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 had 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.

VistA Evolution

In December 2013, VA initiated its VistA Evolution program as a joint effort of VHA and OI&T. 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 is 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.

To expedite the acquisition, in June 2017, the Secretary signed a "Determination and Findings," for a public interest exception[25] 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, the department has estimated that, as of November 2018, an additional $6.1 billion in funding, above the Cerner contract amount, will be needed to fund additional project management support supplied by outside contractors, government labor costs, and infrastructure improvements over a 10-year implementation period.

Deployment of the new electronic health record system at three initial sites is planned for March 2020,[26] with a phased implementation of the remaining sites over the next decade. Each VA medical facility is

[25]FAR, 48 C.F.R. § 6.302-7.

[26]The three initial deployment sites are the Mann-Grandstaff, American Lake, and Seattle VA Medical Centers.

expected to continue using VistA until the new system has been deployed at that location.

After VA announced in June 2017 that it planned to acquire the Cerner electronic health record system, we testified in June 2018 that a governance structure had been proposed that would be expected to leverage existing joint governance facilitated by the Interagency Program Office.[27] At that time, VA's program officials had stated that the department's governance plans for the new program were expected to be finalized in October 2018. However, the officials had not indicated what role, if any, the Interagency Program Office was to have in the governance process. This office has been involved in various approaches to increase health information interoperability since it was established by the National Defense Authorization Act for Fiscal Year 2008 to function as the single point of accountability for DOD's and VA's electronic health record system interoperability efforts.

In September 2018, we recommended that VA clearly define the role and responsibilities of the Interagency Program Office in the governance plans for acquisition of the department's new electronic health record system.[28] The department concurred with our recommendation and stated that the Joint Executive Committee, a joint governance body comprised of leadership from DOD and VA, had approved a role for the Interagency Program Office that included providing expertise, guidance, and support for DOD, VA, and joint governance bodies as the departments continue to acquire and implement interoperable electronic health record systems.

However, the department has not yet provided documentation supporting these actions and how they relate to VA's governance structure for the new acquisition. In addition, the role described does not appear to position the office to be the single point of accountability originally identified in the National Defense Authorization Act for Fiscal Year 2008. We continue to monitor the department's governance plans for the acquisition of the new electronic health record system and its relationship with the Interagency Program Office.

[27]GAO, *VA IT Modernization: Preparations for Transitioning to a New Electronic Health Record System Are Ongoing*, GAO-18-636T (Washington, D.C.: June 26, 2018).

[28]GAO, *Electronic Health Records: Clear Definition of the Interagency Program Office's Role in VA's New Modernization Effort Would Strengthen Accountability*, GAO-18-696T (Washington, D.C.: Sept. 13, 2018).

The Family Caregiver Program Has Not Been Supported by an Effective IT System

In May 2010, VA was required by statute to establish a program to support family caregivers of seriously injured post-9/11 veterans. In May 2011, VHA implemented its Family Caregiver Program at all VA medical centers across the country, offering caregivers an array of services, including a monthly stipend, training, counseling, referral services, and expanded access to mental health and respite care. In fiscal year 2014, VHA obligated over $263 million for the program.

In September 2014, we reported that the Caregiver Support Program office, which manages the program, did not have ready access to the types of workload data that would allow it to routinely monitor the effects of the Family Caregiver Program on VA medical centers' resources due to limitations with the program's IT system—the Caregiver Application Tracker.[29] Program officials explained that this system was designed to manage a much smaller program and, as a result, the system has limited capabilities. Outside of obtaining basic aggregate program statistics, the program office was not able to readily retrieve data from the system that would allow it to better assess the scope and extent of workload problems at VA medical centers.

Program officials also expressed concern about the reliability of the system's data. The lack of ready access to comprehensive workload data impeded the program office's ability to monitor the program and identify workload problems or make modifications as needed. This runs counter to federal standards for internal control which state that agencies should monitor their performance over time and use the results to correct identified deficiencies and make improvements.

We also noted in our report that program officials told us that they had taken initial steps to obtain another IT system to support the Family Caregiver Program, but they were not sure how long it would take to implement. Accordingly, we recommended that VA expedite the process for identifying and implementing a system that would fully support the Family Caregiver Program. VA concurred with our recommendation and subsequently began taking steps to implement a replacement system. However, the department has encountered challenges related to the system implementation efforts. We have ongoing work to evaluate VA's effort to acquire a new IT system to support the Family Caregiver Program.

[29]GAO-14-675.

Additional Actions Can Improve Efforts to Develop and Use the Veterans Benefits Management System

In September 2015, we reported that VBA had made progress in developing and implementing VBMS—its system for processing disability benefit claims—but also noted that additional actions could improve efforts to develop and use the system.[30] Specifically, VBA had deployed the initial version of the system to all of its regional offices as of June 2013. Further, after initial deployment, it continued developing and implementing additional system functionality and enhancements to support the electronic processing of disability compensation claims.

Nevertheless, we pointed out that VBMS was not able to fully support disability and pension claims, as well as appeals processing. While the Under Secretary for Benefits stated in March 2013 that the development of the system was expected to be completed in 2015, implementation of functionality to fully support electronic claims processing was delayed beyond 2015. In addition, VBA had not produced a plan that identified when the system would be completed. Accordingly, holding VBA management accountable for meeting a time frame and demonstrating progress was difficult.

Our report further noted that, even as VBA continued its efforts to complete the development and implementation of VBMS, three areas were in need of increased management attention: cost estimating, system availability, and system defects. We also noted in our report that VBA had not conducted a customer satisfaction survey that would allow the department to compile data on how users viewed the system's performance and, ultimately, to develop goals for improving the system.

We made five recommendations to improve VA's efforts to effectively complete the development and implementation of VBMS. VA agreed with four of the recommendations. In addition, the department has addressed one of the recommendations—that it establish goals for system response time and use the goals as the basis for reporting system performance.

However, the department has not yet fully addressed our remaining recommendations to (1) develop a plan with a time frame and a reliable cost estimate for completing VBMS, (2) reduce the incidence of system defects present in new releases, (3) assess user satisfaction, and (4) establish satisfaction goals to promote improvement. Continued attention to these important areas can improve VA's efforts to effectively complete

[30]GAO-15-582.

the development and implementation of VBMS and, in turn, more effectively support the department's processing of disability benefit claims.

VA Has Demonstrated Uneven Progress toward Implementing Key FITARA Provisions

FITARA included provisions for 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.[31]

VA's progress toward implementing key FITARA provisions has been uneven. Specifically, VA issued a software licensing policy and has generated an inventory of its software licenses to inform future investment decisions. However, the department did not fully address requirements related to IT investment risk, data center consolidation, or CIO authority enhancement.

Software Licensing

VA has made progress in addressing federal software licensing requirements. In May 2014, we reported on federal agencies' management of software licenses and stressed that better management was needed to achieve significant savings government-wide.[32] 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

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

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

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. For example, the department implemented 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; and it subsequently identified approximately $65 million in cost savings over 3 years due to analyzing one of its software licenses.

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 risk ratings assigned to investments by CIOs.[33] We noted that the department had reviewed compliance with risk management practices, but had not assessed active risks when developing its risk ratings.

VA determined its ratings by quantifying and combining inputs such as cost and schedule variances, risk exposure values, and compliance with agency processes. Metrics for compliance with agency processes included those related to program and project management, project execution, the quality of investment documentation, and whether the investment was regularly updating risk management plans and logs.

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. Such approaches did not consider individual risks, such as funding cuts or staffing changes, which detail the probability and impact of pending threats to success. Instead, 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. As a result, we recommended that VA factor active risks into its CIO ratings. We also recommended that the department ensure that these ratings reflect the level of risk facing an

[33]GAO-16-494.

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.

Data Center Consolidation

VA has reported progress on consolidating and optimizing its data centers, although this progress has fallen short of targets set by OMB.[34] Specifically, VA reported a total inventory of 415 data centers, of which 39 had been closed as of August 2017.[35] While the department anticipated another 10 data centers would be closed by the end of fiscal year 2018, these closures fell short of the targets set by OMB. Further, while VA reported $23.61 million in data center-related cost savings and avoidances from 2012 through August 2017, the department did not realize further savings from the additional 10 data center closures.[36]

In addition, as of February 2017, VA reported meeting one of OMB's five data center optimization metrics related to power usage effectiveness. Also, the department's data center optimization strategic plan indicated that VA planned to meet three of the five metrics by the end of fiscal year 2018. Further, while OMB directed agencies to replace manual collection and reporting of metrics with automated tools no later than fiscal year 2018, the department had only implemented automated tools at 6 percent of its data centers.

[34]GAO-18-264.

[35]VA reported this data in its August 2017 inventory update to OMB.

[36]For additional information, see Department of Veterans Affairs, Office of Inspector General, *Lost Opportunities for Efficiencies and Savings During Data Center Consolidation*, 16-04396-44 (Washington, D.C.: Jan. 30, 2019). In January 2019, the VA Office of the Inspector General released a report that concluded VA had not reported a projected 860 facilities as data centers, due to incorrect internal agency guidance on what should be classified as a data center. The department agreed with the report's associated recommendations to develop additional guidance on determining what facilities were subject to OMB's data center optimization initiative and to establish a process for conducting a VA-wide inventory of data centers. The VA Office of Inspector General reports the status of these recommendations as closed, based on actions taken by the department.

We have recommended that VA take actions to address data center savings goals and optimization performance targets identified by OMB.[37] The department has taken actions to address these recommendations, including reporting data center consolidation savings and avoidance costs to OMB and updating its data center optimization strategic plan. However, the department has yet to address recommendations related to areas that we reported as not meeting OMB's established targets, including implementing automated monitoring tools at its data centers.

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.[38] We noted that VA'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, as we had recommended. As of October 2018, a VA official stated that the department was working to draft a policy to address our recommendation, but did not identify time frames for when all activities would be completed.

In January 2018, we reported on the need for agencies to involve CIOs in reviewing IT acquisition plans and strategies.[39] 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

[37]For other reports on data center consolidation, see GAO, *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings*, GAO-14-713 (Washington, D.C.: Sept. 25, 2014); *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 Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*, GAO-17-388 (Washington, D.C.: May 18, 2017); and *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).

[38]GAO-18-148.

[39]GAO-18-42.

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 a May 2018 update, provided a draft process map that depicted its forthcoming acquisition process. However, as of March 2019, this process had not yet been finalized and implemented.

In August 2018, we reported that the department had only fully addressed two of the six key areas that we identified—IT Leadership and Accountability and Information Security.[40] The department had partially addressed IT Budgeting, minimally addressed IT Investment Management, and had not at all 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.

VA's Cybersecurity Management Lacks Key Elements

In December 2018, we reported on the effectiveness of the government's approach and strategy for securing its systems.[41] The federal approach and strategy for securing information systems is prescribed by federal law and policy, including FISMA and the presidential executive order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[42]

Accordingly, federal reports describing agency implementation of this law and policy, and reports of related agency information security activities, indicated VA's lack of effectiveness in its efforts to implement the federal approach and strategy. Our December 2018 report identified that the department was deficient or had material weaknesses in all four indicators of departments' effectiveness in implementing the federal

[40]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.

[41]GAO-19-105.

[42]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).

approach and strategy for securing information systems. Specifically, VA was not effective in the Inspector General Information Security Program Ratings, was found to have material weaknesses in the Inspector General Internal Control Deficiencies over Financial Reporting, did not meet CIO Cybersecurity Cross-Agency Priority Goal Targets, and had enterprises that were at risk according to OMB Management Assessment Ratings.

High-Impact Systems

We reported on federal high-impact systems—those that hold sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harm—in May 2016.[43] We noted that VA had implemented numerous controls, such as completion of risk assessments, over selected systems. However, the department had not always effectively implemented access controls, patch management, and contingency planning to protect the confidentiality, integrity and availability of these high-impact systems. These weaknesses existed in part because the department had not effectively implemented elements of its information security program.

We made five recommendations to VA to improve its information security program. The department concurred with the recommendations and, as of March 2019, had implemented three of the five recommendations.

Cybersecurity Workforce

Our March 2019 report on the federal cybersecurity workforce indicated that VA was not accurately categorizing positions to effectively identify critical staffing needs.[44] The Federal Cybersecurity Workforce Assessment Act of 2015 required agencies to assign the appropriate work role codes to each position with cybersecurity, cyber-related, and IT functions. Agencies were to assign a code of “000” only to positions that did not perform IT, cybersecurity, or cyber-related functions.

As we reported, VA had assigned a “000” code to 3,008 (45 percent) of its 6,636 IT positions. Human resources and IT officials from the department stated that they may have assigned the “000” code in error and that they had not completed the process to validate the accuracy of their codes.

We recommended that VA take steps to review the assignment of the "000" code to any of the department’s positions in the IT management

[43]GAO-16-501.

[44]GAO-19-144.

occupational series and assign the appropriate work role codes. VA concurred with the recommendation and indicated that it was in the process of conducting a cyber coding review.

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. In this regard, VA is set to begin deploying its new electronic health record system in less than 1 year and questions remain regarding the governance structure for the program. Thus, it is more important than ever for the department to ensure that it is managing its IT budget in a way that addresses the challenges we have identified in our previous reports and high-risk updates. If the department continues to experience the challenges that we have previously identified, it may jeopardize its fourth attempt to modernize its electronic health record system.

Additionally, the department has been challenged in fully implementing provisions of FITARA, which has limited its ability to improve its management of IT acquisitions. Until the department implements the act's provisions, Congress will be unable to effectively monitor VA's progress and hold it accountable for reducing duplication and achieving cost savings. 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 pursue modernization efforts, it is critical that the department take steps to adequately secure its systems.

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

GAO Contact and Staff Acknowledgments

If you or your staffs 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 testimony statement. GAO staff who made key contributions to this testimony are Mark Bird (Assistant Director), Eric Trout (Analyst in Charge), Justin Booth, Rebecca Eyler, Katherine Noble, Scott Pettis, Christy Tyson, and Kevin Walsh.

(103438)