United States Government Accountability Office

Testimony

Before the Subcommittees on Economic Opportunity and Technology Modernization, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, September 16, 2020

VETERANS AFFAIRS

VA Needs to Address Persistent IT Modernization and Cybersecurity Challenges

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

September 16, 2020

VETERANS AFFAIRS

VA Needs to Address Persistent IT Modernization and Cybersecurity Challenges

Highlights of GAO-20-719T, a testimony before the Subcommittees on Economic Opportunity and Technology Modernization, Committee on Veterans' Affairs, House of Representatives

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—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, which could jeopardize its ability to effectively support key programs such as the Forever GI Bill. GAO has previously reported on these IT management challenges at VA.

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, a system for the Family Caregiver Program, and VBMS; (2) implementing FITARA; and (3) addressing cybersecurity issues. In developing this testimony, GAO reviewed its recently issued reports that addressed IT management issues at VA and GAO's biannual high-risk series. GAO also incorporated information 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, implementation of key FITARA provisions, and cybersecurity program. VA has generally agreed with the recommendations and has begun to address them.

View GAO-20-719T. 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 challenges in its efforts to accomplish three critical information technology (IT) modernization initiatives: the department's health information system, known as the Veterans Health Information Systems and Technology Architecture (VistA); a system for the Family Caregiver Program, which is to support family caregivers of seriously injured post-9/11 veterans; and the Veterans Benefits Management System (VBMS) that collects and stores information and is used for processing disability benefit claims. Specifically,

- GAO has reported on the challenges in the department's three previous unsuccessful attempts to modernize VistA over the past 20 years. However, VA has recently deployed a new scheduling system as part of its fourth effort to modernize VistA and the next deployment of the system, including additional capabilities, is planned in October 2020.
- VA had taken steps to address GAO's recommendations from its 2014 report to implement a replacement system for the Family Caregiver Program. However, in September 2019, GAO reported that VA had yet to implement a new IT system that fully supports the Family Caregiver Program and that it had not yet fully committed to a date by which it will certify that the new IT system fully supports the program.
- In September 2015, GAO reported that VA had made progress in developing and implementing VBMS, but also noted that additional actions could improve efforts to develop and use the system. For example, VBMS was not able to fully support disability and pension claims, as well as appeals processing. GAO made five recommendations aimed at improving VA's efforts to effectively complete the development and implementation of VBMS; however, as of September 2020, VA implemented only one recommendation.

VA's progress in implementing key provisions of the Federal Information Technology Acquisition Reform Act (commonly referred to as FITARA) has been uneven. Specifically, VA has made progress toward improving its licensing of software and achieving its goals for closing unneeded data centers. However, the department has made limited progress toward addressing requirements related to IT investment risk management and Chief Information Officer authority enhancement. Until the department 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 will be hindered.

In addition, since fiscal year 2016, GAO has reported that VA faces challenges related to effectively implementing the federal approach to, and strategy for, securing information systems; effectively implementing information security controls and mitigating known security deficiencies; and establishing elements of its cybersecurity risk management program. GAO's work stressed the need for VA to address these challenges as well as manage IT supply chain risks. As VA continues to pursue modernization efforts, it is critical that the department take steps to adequately secure its systems.

Chairs Lee and Levin, Ranking Members Banks and Bilirakis, and Members of the Subcommittees:

Thank you for the opportunity to participate in today's hearing regarding the modernization of education services at the Department of Veterans Affairs (VA). The department provided about $11.7 billion in education benefits in fiscal year 2019 to about 23,000 schools to provide approved programs of education and training to eligible veterans and their beneficiaries and help them afford postsecondary education.

As you know, the use of information technology (IT) is crucial to helping VA effectively serve the nation's veterans, including those who receive education benefits. 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 its Office of Information and Technology (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 VA's efforts in (1) modernizing VistA, a system for the Family Caregiver Program, and the Veterans Benefits Management System (VBMS); (2) implementing FITARA; and (3) addressing cybersecurity issues.

In developing this testimony, we reviewed our recently issued reports on VA's efforts to modernize systems, to implement FITARA, and to address cybersecurity weaknesses and our biannual 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

[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).

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 specialized care, and it performs research and development to address veterans' needs. Further, NCA provides burial and memorial benefits to veterans and their families.

More specifically, with respect to education benefits provided by VBA, eligible individuals could receive payments to cover education costs. The Colmery Act (also referred to as the "Forever GI Bill"), enacted in August 2017, changed education benefits available to veterans, service members, families and survivors, including eliminating the time limit on the use of Post-9/11 GI Bill benefits, expanding eligibility for benefits, and modifying certain benefit amounts.[4]

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

[4]Harry W. Colmery Veterans Educational Assistance Act of 2017 (Colmery Act), Pub. L. No. 115-48, Title III, § 311, 131 Stat. 973, 995 (Aug. 16, 2017).

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.

VBA relies on VBMS to process disability claims and to collect and store information such as military service records, medical examinations, and treatment records from VA, the Department of Defense (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.

In addition, 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.

In June 2017, the former VA Secretary announced that the department planned to acquire the same Cerner electronic health record system that 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.

[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.

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 2020, OI&T was comprised of over 16,000 government and contract staff.

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

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

[7]GAO-15-290.

[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.[10]

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.[11] 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.

Our March 2019 update to our 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 area.[12] The capacity, monitoring, and demonstrated progress criteria remained unchanged.

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

[10]GAO-17-317.

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

[12]GAO-19-157SP.

achieving cost savings. The law applies to VA and other covered agencies.[13]

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.[14]

- **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 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 requires OMB to develop a goal for how much is to be saved through this initiative, and provide annual reports on cost savings achieved.[15]

[13]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.

[14]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.

[15]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, 2022. Pub. L. No. 115-88 (Nov. 21, 2017).

- **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.[16] Additionally, in the case of major investments rated as high risk for 4 consecutive quarters,[17] 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.[18]

In June 2015, OMB released guidance describing how agencies are to implement FITARA.[19] 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

[16]"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.

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

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

[19]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 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.[20] 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*,[21] 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*[22] (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.

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.

[20]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.

[21]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).

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

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.[23]

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 2019 annual FISMA report to Congress, agencies reported 28,581 information security incidents to DHS's U.S. Computer Emergency Readiness Team[24] in fiscal year 2019.

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

VA has faced longstanding challenges in its efforts to accomplish three critical IT modernization initiatives: VistA, the Family Caregiver Program, and VBMS. Specifically, after three unsuccessful attempts to modernize VistA, the department has initiated a fourth effort. 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 Initiated Its Fourth Effort to Modernize VistA

VA has pursued four efforts over nearly 2 decades to modernize VistA.[25] 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.

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

[23]GAO-19-157SP.

[24]Within the Department of Homeland Security, 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.

[25]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).

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.[26] In June 2009, the Secretary of VA 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

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 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 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

[26]GAO-08-805.

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[27] 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 began in August 2020 with the deployment of a new scheduling solution at the VA Central Ohio Healthcare System. The next deployment of the system, including additional capabilities, is planned at the Mann-Grandstaff VA Medical Center in Spokane, Washington, in October 2020, 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. We have ongoing work in which we are continuing to monitor VA's progress toward deploying its new electronic health record system.

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

[27]FAR, 48 C.F.R. § 6.302-7.

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 (CAT).[28] 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.

In September 2019, we reported that VA had yet to implement a new IT system that fully supported the Family Caregiver Program as required by the VA MISSION Act of 2018.[29] VHA and OI&T had been working jointly on projects since 2015 to improve and replace CAT. However, two of these projects were terminated without delivering viable software improvements or a replacement system. According to two independent assessments, these prior efforts lacked both effective leadership and implementation of the processes needed for requirements management.

[28]GAO-14-675.

[29]The VA MISSION Act of 2018, enacted in June 2018, requires the expansion of Family Caregiver Program eligibility to include caregivers of veterans who served prior to September 11, 2001. Pub. L. No. 115-182, §§ 161-163, 132 Stat. 1438-1443 (2018). GAO, *VA Health Care: Actions Needed to Improve Family Caregiver Program,* GAO-19-618 (Washington, D.C.: Sept. 16, 2019).

VA has asserted that its third project, in which OI&T and VHA have begun to acquire and implement a commercial product to replace CAT, will take steps to avoid the issues that impacted its past efforts. In July 2020, the department reported that the first two phases of the new system, the Caregiver Record Management Application (CARMA), had been deployed.

Nevertheless, the Caregiver Support Program remains dependent on the successful delivery of additional system releases for increased functionality, which have not yet occurred. The third phase of the system implementation, which had been expected to be complete in the summer of 2020, is now targeted for October 2020. However, the department has not yet fully committed to a date by which it will certify that the new IT system fully supports the program. Until CARMA is fully implemented and certified by the Secretary of VA, it is unclear if the expansion of eligibility for the Family Caregiver Program will be adequately supported by the new system.

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 had 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

[30]GAO-15-582.

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 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.

Further, VA took limited actions in response to our recommendations that it assess user satisfaction and establish satisfaction goals to promote system improvement. Also, the department did not ensure the statistical validity of its user satisfaction survey and does not plan to establish user satisfaction goals for VBMS.

In addition, the department has not yet implemented our recommendations to (1) develop a plan with a time frame and a reliable cost estimate for completing VBMS and (2) reduce the incidence of system defects present in new releases. Continued attention to these important areas can improve VA's efforts to effectively complete 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 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.[31]

VA's progress in implementing key FITARA provisions has been uneven. Specifically, VA has made progress toward improving its licensing of software. However, the department has had mixed results toward achieving its data center consolidation goals, while it has made limited progress in addressing requirements related to IT investment risk and CIO authority enhancement.

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

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 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

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

[33]GAO-16-494.

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 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; however, as of September 2020, these recommendations remained not implemented.

Data Center Consolidation

VA has reported progress on consolidating and optimizing its data centers. Specifically, the department reported that it planned to meet its fiscal year 2019 target for data center closures. In particular, VA set a target to close 14 of its 309 data centers during fiscal year 2019. As of August 2019, the department had closed 12 data centers with an additional 11 planned closures expected to bring the total number of data centers at the end of fiscal year 2019 to 286.[34]

Further, while VA reported $23.61 million in data center-related cost savings and avoidances from 2012 through August 2017, the department

[34]GAO, *Data Center Optimization: Agencies Report Progress, but Oversight and Cybersecurity Risks Need to be Address,* GAO-20-279 (Washington, D.C.: Mar. 5, 2020).

did not realize further savings from the fiscal year 2019 data center closures. Specifically, VA did not report any fiscal year 2019 cost savings because the majority of those data centers were within multi-use facilities that were still owned and maintained by the agency. However, the department plans to achieve cost savings in fiscal year 2020 because it expects to stop leasing two data centers, which is expected to reduce data center spending.

In addition, as of September 2019, VA reported meeting two of OMB's four data center optimization metrics related to virtualization and server utilization.[35] However, the department did not meet OMB's target for advanced energy metering. VA officials reported that they did not meet the advanced energy metering target due to difficulties in getting a contract in place to install the metering. Further, we determined that OMB's data center availability metrics were not sufficiently reliable for us to report progress for that metric.

We have recommended that VA take actions to fully address data center targets identified by OMB.[36] 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.

[35]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.

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

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.[37] 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 September 2020, 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.[38] 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, VA issued a Standard Operating Procedure that required the CIO and Chief Acquisition Officer to work in conjunction to review and approve all IT acquisition strategies and plans. However, the department had not provided evidence that the CIO (or designee) was reviewing and approving selected IT acquisition plans.

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.[39] The department had partially

[37]GAO-18-148.

[38]GAO-18-42.

[39]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.

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 September 2020, the department has not addressed this recommendation.

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 challenges relate to the department effectively implementing the federal approach and strategy for securing information systems, effectively implementing 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 Security Information Systems

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.[40] In December 2018, we reported on the effectiveness of the government's approach and strategy for securing its systems.[41] Our report pointed out that the department was deficient or had material weaknesses in all four indicators of its effectiveness in implementing the federal approach and strategy for securing information systems. Specifically, we noted that 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

[40]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).

[41]GAO-19-105.

Cybersecurity Cross-Agency Priority Goal Targets; and had enterprises that were at risk, according to OMB Management Assessment Ratings.

Effectively Implementing Information Security Controls and Mitigating Known Security Deficiencies

VA has been challenged to effectively implement 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, 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 August 2020, VA had implemented 55 (or 74 percent) of the 74 recommendations. One of the remaining unimplemented recommendations calls for the department to conduct security control assessments and ensure the procedures comprehensively test technical controls. This recommended activity is an important element of a cybersecurity program and helps to provide assurance that controls are operating as intended and to detect controls that are not functioning correctly. Until VA rectifies reported shortcomings in its department-wide information security program, it will continue to have limited assurance that its sensitive information and information systems are sufficiently safeguarded.

[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.

[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).

Fully Establishing Elements of a Cybersecurity Risk Management Program

VA has been challenged in managing its cybersecurity risk. 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 asserted that it is acting to do so. Nevertheless, 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. In July 2018, we reported that reliance on a global IT supply chain introduces risks to federal information systems.[46] We noted that supply chain threats are present during various phases of a system's development life cycle and we identified the following threats:

- installation of malicious or intentionally harmful hardware or software;
- installation of counterfeit hardware or software;

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

[46]GAO-18-667T.

- failure or disruption in the production or distribution of critical products;
- reliance on a malicious or unqualified service provider; and
- installation of hardware or software that contains unintentional vulnerabilities, such as defects in code that can be exploited.

These threats can have a range of impacts, including allowing adversaries to take control of systems or decreasing the availability of materials or services needed to develop systems.

Accordingly, it is critical for agencies, including VA, to take appropriate measures to assess and manage IT supply chain risks as they operate and modernize their information systems. Failure to do so could result in data loss, modification, or exfiltration; loss of system availability; and a persistent negative impact on the agency's mission.

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. Thus, it is more important than ever for the department to ensure that it is managing its IT 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 ability to effectively support key programs, such as the Forever GI Bill.

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 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 will be hindered.

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.

Chairs Lee and Levin, Ranking Members Banks and Bilirakis, and Members of the Subcommittees, 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 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 statement. GAO staff who made key contributions to this testimony are Mark Bird (Assistant Director), Christy Tyson (Analyst in Charge), Justin Booth, Rebecca Eyler, Valerie Hopkins, Tammi Kalugdan, Jeff Knott, George Kovachick, Scott Pettis, Jennifer Stavros-Turner, Eric Trout, and Kevin Walsh.