MAPPING THE CHALLENGES AND PROGRESS OF THE OFFICE OF INFORMATION AND TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

OF THE

COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

TUESDAY, APRIL 2, 2019

Serial No. 116–2

Printed for the use of the Committee on Veterans' Affairs

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
38–952 WASHINGTON : 2021

COMMITTEE ON VETERANS' AFFAIRS

MARK TAKANO, California, *Chairman*

JULIA BROWNLEY, California
KATHLEEN M. RICE, New York
CONOR LAMB, Pennsylvania, *Vice-Chairman*
MIKE LEVIN, California
MAX ROSE, New York
CHRIS PAPPAS, New Hampshire
ELAINE G. LURIA, Virginia
SUSIE LEE, Nevada
JOE CUNNINGHAM, South Carolina
GILBERT RAY CISNEROS, JR., California
COLLIN C. PETERSON, Minnesota
GREGORIO KILILI CAMACHO SABLAN, Northern Mariana Islands
COLIN Z. ALLRED, Texas
LAUREN UNDERWOOD, Illinois
ANTHONY BRINDISI, New York

DAVID P. ROE, Tenessee, *Ranking Member*
GUS M. BILIRAKIS, Florida
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
MIKE BOST, Illinois
NEAL P. DUNN, Florida
JACK BERGMAN, Michigan
JIM BANKS, Indiana
ANDY BARR, Kentucky
DANIEL MEUSER, Pennsylvania
STEVE WATKINS, Kansas
CHIP ROY, Texas
W. GREGORY STEUBE, Florida

RAY KELLEY, *Democratic Staff Director*
JON TOWERS, *Republican Staff Director*

SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

SUSIE LEE, Nevada, *Chairwoman*

JULIA BROWNLEY, California
CONOR LAMB, Pennsylvania
JOE CUNNINGHAM, South Carolina

JIM BANKS, Indiana, *Ranking Member*
STEVE WATKINS, Kansas
CHIP ROY, Texas

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Veterans' Affairs are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

Tuesday, April 2, 2019

MAPPING THE CHALLENGES AND PROGRESS OF THE OFFICE OF INFORMATION AND TECHNOLOGY

Tuesday, April 2, 2019

COMMITTEE ON VETERANS' AFFAIRS,
U. S. HOUSE OF REPRESENTATIVES,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:20 a.m., in Room 1302, Longworth House Office Building, Hon. Susie Lee presiding.

Present: Representatives Lee, Brownley, Lamb, Cunningham, Banks, Watkins, and Roy.

OPENING STATEMENT OF SUSIE LEE, CHAIRWOMAN

Ms. LEE. Good morning. This hearing will now come to order.

This is the first hearing of the 116th Congress by the Subcommittee on Technology Modernization. This Subcommittee was created last year and recognized that all aspects of implementing technology at the Department of Veterans Affairs needs to be sustained attention and oversight.

I am pleased that the work that was begun last year will continue and I am honored to be part of the effort. I look forward to working with my colleague, Ranking Member Banks, and the other Members of the Subcommittee on this very important mandate.

VA has many technology modernization projects underway, from the Electronic Health Record Modernization, the Financial Management Business Transformation, and the efforts to update its supply chain system.

Congress has also given VA several critical programs to implement, including the MISSION Act and the Forever GI Bill. These programs will need to have strong technology systems that support the successful delivery of health care and benefits to our veterans. The Subcommittee will engage in oversight of each of these programs over the next several months; however, I thought it would be helpful to begin the Subcommittee's work with an assessment of the office within the VA that bears much of the responsibility for implementing that technology that will support these critical programs.

The Office of Information and Technology, I will refer to as OIT, is responsible for all aspects of technology modernization in the VA, including the acquisition, development, and implementation.

OIT is also responsible for making sure that VA's critical systems are secure, and that veterans' personal data is protected.

It is clear that OIT has struggled in its mission. Many decades of oversight by the Government Accountability Office and the Office of Inspector General have found and documented systematic leadership and management challenges at OIT. Progress at solving these problems, unfortunately, has been halting. Today, I would like to explore the root causes of these challenges and to identify the barriers for improvement. And if OIT has made progress, I would like to explore that as well, so that we can determine how to successfully replicate those results.

One of the major problems at OIT has been high turnover in leadership. VA has had five Chief Information Officers in 4 years. I am glad that the confirmed leader is in place and I wish Mr. Gfrerer success in his position, and I hope that he is able to implement some of the critical change that is needed at OIT. However, you will note that we have an empty chair at the table where OIT should be represented. The Subcommittee invited Mr. Gfrerer to the hearing today, but the VA declined, because he is testifying before the Full Committee later this afternoon. That is somewhat understandable, and we told the VA we would accept a Deputy for testimony today.

I want to be clear that we won't stand on ceremony in the Subcommittee. We want to engage with knowledgeable management and staff, no matter their title, to better understand these challenges and figure out the solutions. Unfortunately, VA refused this Subcommittee's request.

I hope we will hear from OIT at a Subcommittee hearing in the near future, because if we want VA to be able to successfully deliver health care and benefits to our veterans, OIT has to be an effective part of that effort.

There is no doubt that we want OIT to succeed at its mission, because its success means that veterans get the highest level of care and reliable access to the benefits they have earned.

I am pleased to have Members of our oversight community here today to help the Subcommittee further its oversight of technology at VA. I look forward to testimony from the GAO and OIG, and engaging in discussion with them now and moving forward.

Thank you.

Ms. LEE. I would now like to recognize my colleague Ranking Member Banks for 5 minutes to deliver any opening remarks he may have.

Mr. Banks.

OPENING STATEMENT OF JIM BANKS, RANKING MEMBER

Mr. BANKS. Thank you, Madam Chair. It is my privilege to be working with you on this Subcommittee this Congress.

We got off to a great start with oversight of the HR Modernization Program last year; that continues to be my priority, but our jurisdiction extends to all enterprise technology projects, and I commend you for considering other issues as well.

The VA Office of Information and Technology is responsible for the networks, computers, and software that VBA, VHA, and NCA rely on to carry out their missions. I was relieved to see the Chief Information Officer, Mr. Gfrerer, confirmed by the Senate on the very last day of the 115th Congress. We had a candid, encouraging

meeting in my office last month and I look forward to working with him.

I understand that Mr. Gfrerer will be testifying before the Full Committee this afternoon, but I was surprised and, frankly, disappointed that not only was he unable to appear this morning, but VA declined to send any witness in his place from OIT. I was hoping to start this year with a discussion of OIT's activities and priorities. I appreciate the Secretary outlining his focuses: EHRM, the MISSION Act, supply chain integration with DoD, and financial systems modernization; given the circumstances, I am going to take this opportunity to outline mine.

VA's number one IT problem, before we even get into specific programs, is that operation and maintenance of legacy systems and fixed infrastructure cost consume almost all of the OIT budget. When I joined this Committee, that percentage was about 80, and now it is approaching 90. We have been devoting more attention to IT, but the situation is actually getting worse.

The Administration is proposing a $240 million OIT increase on a base of about $4.1 billion. I agree, we have to invest in IT, but I need to know this will actually bend that cost curve and produce some new capabilities rather than perpetuate the current state of affairs.

As to EHRM, OIT's role is upgrading the networks and computer hardware at the medical centers in anticipation of Cerner being installed. I am cautiously optimistic that OIT is actually ahead of the curve here. Although OIT's role has not changed, VA has decided to shift many of these infrastructure costs out of the EHRM appropriation into the OIT appropriation. I do not object to that in principle, but I am concerned about transparency.

As to the MISSION Act IT systems, chiefly the Decision Support Tool, I appreciate the media bringing attention to the issue, but we are getting a lot of alarming conjecture without the basic information about what the projects are and what they are supposed to do. I look forward to discussing that in this afternoon's hearing.

As to the VA adopting DMLSS from DoD and integrating the supply chains, I generally agree with the concept, but I have been given very little information on which to base an opinion. The Subcommittee needs an in-depth briefing on the pilot site, and we know to know the long-term plan. I think adding DMLSS to the EHRM scope of work in Spokane and Seattle might be one too many blocks on the Jenga tower.

I will say that I am concerned about what impact the cost of these new systems for the MISSION Act, supply chain, and others will have on bending that operations and maintenance cost curve.

DST is a new system integrating data from a half a dozen legacy systems and it is going to layer on top of them, not replace any of them. Integrating DST with CPRS is messy and difficult, and the whole goal of EHRM is to get rid of CPRS. DMLSS has existed in DoD for a long time, but is going to be a complicated integration into VA. I see a natural tension here between adding new systems that are necessary to VA's mission and retiring old systems to bend that cost curve.

Finally, as to the Financial Management Business Transformation Program, I need to see some forward movement. VA

started FMBT almost 3 years ago and I have watched it relaunch three separate times, balloon in cost to above $2 billion, but not deliver any new capabilities. We have been told that the old financial and accounting software barely holds together, and VA's ability to pass an audit is hanging on by a thread; that sort of thing absolutely gets my attention, but FMBT stalls and the status quo seems to continue without incident. That makes me question the urgency that VA used to sell this program.

I appreciate our witnesses from OIG and GAO being here and I am eager to hear your perspectives. And with that, Madam Chair, I yield back.

Ms. LEE. Thank you, Mr. Banks.

I will now introduce the witnesses that have come before the Subcommittee today. First, I would like to introduce Carol Harris, who is the Director of Information Technology Acquisition Management Issues at the U.S. Government Accountability Office.

Brent Arronte is the Deputy Assistant Inspector General in the Office of Audits and Evaluations in the VA Office of the Inspector General, and he is accompanied by Michael Bowman, who is the Director of Information Technology and Security Audits Division within the Office of Inspector General. Welcome.

We will now hear the prepared statements from our panel Members. Your written statements in full will be included in the hearing record without objection.

Ms. Harris, you are recognized for 5 minutes.

STATEMENT OF CAROL HARRIS

Ms. HARRIS. Thank you, Madam Chairlady.

Chair Lee, Ranking Member Banks, and Members of the Subcommittee, thank you for inviting us to testify today on the state of IT acquisitions and operations at VA. As requested, I will briefly summarize our prior work on the Department's systems modernization efforts over the last decade, as well as its IT acquisition reform and cyber security efforts.

As you know, the use of IT is crucial to helping VA effectively serve the Nation's veterans. Each year the Department spends billions of dollars on its information systems and assets. VA's IT budget now exceeds $4 billion annually. This morning I would like to highlight three key points from our body of IT-related work at VA.

First, VA's management of IT system modernization efforts continues to be high risk. VA's track record of delivering failed or troubled IT systems is a large part of why we designated VA health care as a high-risk area for the Federal Government in 2015.

For example, VA pursued three efforts over nearly two decades to modernize VistA, its health information system. These efforts experienced high costs, challenges to ensuring interoperability of health data, and ultimately did not result in a modernized system. VA recently initiated its fourth effort, called the Electronic Health Record Modernization, and the program is already facing serious challenges.

As we have previously reported, the Government's plan for this program has not been fully defined, nor has the VA fully imple-

mented our recommendation to define a role of the key office in its governance plans.

VA's Veterans Benefits Management System, its system for processing disability benefit claims, we pointed out that the system was not able to fully support disability and pension claims, as well as appeals processing. The development of this system was expected to be completed in 2015, but that did not occur, and VA had not produced a plan that identified when the system would be completed.

We also noted three areas that were in need of increased management attention: cost estimating, system availability, and system defects. Accordingly, we made five recommendations to improve VA's ability to more effectively complete and deliver the system. The Department has only addressed one of the five recommendations thus far.

My second point, VA's progress to better manage its IT operations is uneven and its CIO authorities continue to have key weaknesses.

I am pleased to report that the Department has implemented a comprehensive software license management program based on six recommendations we made in 2014. As a result, VA is able to analyze agency-wide software license data such as usage and costs, and it subsequently identified about $65 million in cost savings over 3 years from analyzing just one of its licenses. However, progress is much more limited when it comes to accurately assigning risk to VA's IT investment portfolio, as well as meeting OMB's targets for data center closures and optimization.

The Department also lacks policies fully addressing the role and responsibilities of the CIO in four of six statutory areas, including IT workforce and budgeting. Ensuring that these CIO authorities are formalized is especially critical for the Department, as they have had ten CIOs since 2004 and six since 2012, thus making the average CIO tenure at VA less than 2 years.

Lastly, in the area of cyber security, VA has more work to ensure its high-impact systems are adequately protected. These systems hold sensitive information, the loss of which could cause a Nation catastrophic harm. In May 2016, we found VA had implemented a number of security controls over selected systems, but that it had also not always effectively implemented access controls, patch managements, and contingency planning to protect the confidentiality, integrity, and availability of these critical systems. These weaknesses existed in part because VA lacked a robust information security program.

Moving forward in these three areas I noted, it will be critical for VA to fully and effectively implement our 17 open recommendations as soon as possible. Doing so will better position the Department to more effectively deliver secure systems and IT operations that meet mission needs, and also, where available, realize additional cost savings.

That concludes my statement. I look forward to addressing your questions.

[THE PREPARED STATEMENT OF CAROL HARRIS APPEARS IN THE APPENDIX]

Ms. LEE. Thank you, Ms. Harris.

Mr. Arronte, you are now recognized for 5 minutes.

STATEMENT OF BRENT ARRONTE

Mr. ARRONTE. Thank you, Madam Chair, Ranking Member Banks, and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's oversight of VA's Office of Information and Technology.

VA faces challenges in developing IT systems it needs to support its current goals and overall mission. For over 20 consecutive years, information security has been reported as a material weakness in VA's consolidated financial statement audit. Our audits have shown that IT systems development and management at the VA is a long-standing, high-risk challenge. Despite some incremental advances, our reports indicate VA IT programs are still often susceptible to cost overruns, schedule slippages, and performance problems.

Further, VA struggles to maintain a permanent CIO. Since June of 2013, VA has had six permanent or acting CIOs. From January 2017 to January 2019, there have been three acting CIOs. With such turnover in a key position, it is difficult for VA to support and drive IT innovation for the Department.

In fiscal year 2016, the VA's Chief Information Officer formed an Enterprise Cyber Security Strategy Team, also known as ECST, that developed an Enterprise Cyber Security Strategic Plan. The plan was designed to help VA achieve transparency and accountability, while securing veteran information through teamwork and innovation. The team scope included management of current cyber security efforts, as well as the development and review of VA's operational requirements from desktop to software to network protection.

The ECST has launched 31 plans of action to address previously identified weaknesses. We continue to see information systems security deficiencies similar in type and risk level to our findings in prior years, and an overall inconsistent implementation of the security program.

Our annual FISMA audits indicate that the Enterprise Cyber Security Plan efforts has not been fully effective in addressing or eliminating material weaknesses found in VA's information security program for fiscal year 2018.

Examples of some of those weaknesses identified are legacy financial management system, password standards not consistently implemented, and users provided inappropriate access to some systems, and systems not securely configured to mitigate vulnerabilities.

VA is also challenged in developing IT systems needed to support mission goals. Recent OIG reports disclose that some progress has been made in timely deploying system functionality because of the agile system development methodology. However, despite these incremental advances, VA struggles with cost overruns and performance shortfalls in its efforts to develop several major mission-critical systems.

VA's mechanism for overseeing IT program management has improved, but has not been fully effective in controlling these IT investments.

Our work has demonstrated that VA continues to struggle with its IT investments and securing IT systems. Some improvements in information security management have become evident with the inception of the ECST initiative; however, more work remains to be done and VA needs to remain focused on addressing OIG recommendations in the security and development of IT systems. Until a proven process is in place to ensure control across the enterprise, the IT material weaknesses may stand, and VA's mission-critical systems and sensitive veterans' data may remain at risk of attack or compromise.

Madam Chair, this concludes my statement. We would be happy to answer any of your questions or questions from other Members of the Committee.

[THE PREPARED STATEMENT OF BRENT ARRONTE APPEARS IN THE APPENDIX]

Ms. LEE. Thank you very much, Mr. Arronte.

We will now begin the question-and-answer portion of the hearing, and I would like to start by asking a few questions of Ms. Harris from the GAO.

The GAO has included the VA on its high-risk list since 2015, at least partially because of the information technology struggles. In your report to congressional committees in March of 2019, GAO found that the VA had regressed in the area of leadership commitment.

Will you explain GAO's views on why this rating changed for the worse?

Ms. HARRIS. Yes, ma'am. So the reason why VA regressed in this area is because of the frequent turnover in the CIO leadership. Again, the average turnover—or the average tenure of the VA CIO is less than 2 years and that is a major problem.

Our work has shown that the CIO needs to be in office roughly 3 to 5 years to be effective, and about 5 to 7 years for any major change initiative to take hold in a large public sector organization.

And so that is the primary reason as to why VA regressed in that area.

Ms. HARRIS. Thank you.

What is the status of the VA's efforts to address the recommendations that the GAO had made in relation to VA's IT management issues?

Ms. HARRIS. Well, we have made 29 recommendations in total related to the IT management challenges, VA has closed roughly 40 percent of those recommendations thus far, so there are about 60 percent that are remaining. And so those are related to the disability benefits system and ensuring that they have a plan in place for when they intend to complete the remaining functionality for that system. That is one of the priority recommendations that we have identified.

Another priority recommendation that we believe VA should implement as soon as possible is defining the role of the Interagency

Program Office on its Electronic Health Records Modernization Program, and they should do that as soon as possible.

And then the last priority recommendation of that remaining 60 percent that are open are related to data center optimization, because, as Mr. Banks had noted, you know, 80 percent of the IT OI&T budget is mired in that legacy system money. And so to identify areas where there can be cost savings, data center optimization is one of those areas where cost savings in that area could be reinvested into developing new modernized systems.

Ms. LEE. How many of—speaking of those top priorities in your recommendations, how many of those require the leadership of the CIO?

Ms. HARRIS. All three areas require the leadership of the CIO. I mean, certainly in the area of the Electronic Health Records Modernization, the CIO doesn't play the primary role, he is more of a supporting role for the Department, but his leadership still needs to be there, because he will be responsible for the infrastructure that is necessary for when that system is deployed.

Ms. LEE. Thank you.

Mr. Arronte, in your recent report on the Forever GI Bill implementation, you found that no one appeared to be in charge of the project. This seems to, unfortunately, be a common theme at the VA. What were your findings regarding the lack of accountability?

Mr. ARRONTE. Yes, ma'am. We found there was no single accountable management official. And what happened—and we agree with you, this seems to be a common theme, and what happens is, when it is time to make final decisions about an initiative or an application, there is nobody there to do that. So it stalls the initiative, the initiatives tend to be pushed out the door when they are not ready, and then what we end up seeing is functionality problems with those programs as they mature. And then they try to fix it in flight, so to speak, and they struggle with that.

I think they struggle with program management across the board when it comes to IT initiatives.

Ms. LEE. In your opinion, why do you think the VA has found it so difficult?

Mr. ARRONTE. Without trying to speculate too much, based on our experience, I think there is just—maybe this is a poor analogy—maybe there are too many chefs in the kitchen, and everybody has ownership of a piece of this, and I think there is poor communication between the CIO's office and the administrations.

Ms. LEE. Thank you very much.

I now yield 5 minutes to Mr. Banks for his questions.

Mr. BANKS. Thank you, Madam Chair.

Ms. Harris, the last time you testified before the Subcommittee, we were talking about the IPO, the Interagency Program Office, and the management of EHRM and MHS Genesis. Everyone agreed the IPO is not living up to Congress' vision for a single point of accountability. At the time, I promised legislation on the subject. Unfortunately, DoD and VA still have not come to any decisions.

Last week, staff began circulating a summary of the legislation, we are working to finalize it. The idea is the IPO should be repurposed to organize all aspects of interoperability, not just the

electronic health records, between DoD, VA, and the Office of the National Coordinator. The departments will have to figure out what level of centralized control they want, but we need to focus on comprehensive interoperability.

What more can you add today about the IPO's role and what is your opinion of the concept of that type of legislation?

Ms. HARRIS. I appreciate the question, Mr. Banks. I think the IPO, as it is currently operating, is not an effective office for leading or for being that central point of accountability. I think you have two departments, VA and DoD, who are unwilling to relinquish control to a third party to make those decisions. And I think that this is actually the most important recommendation that we have made for the EHRM program. If DoD and VA cannot formalize a process for how they are going to adjudicate these really tough issues, they are going to fail again in this fourth attempt in integrating their systems.

So, again, having a single point of accountability is crucial, because when the wheels start falling off the bus, we have to be able to identify who is responsible in order to effectively have corrective actions.

And in terms of the proposed legislation, we are happy to take a look at it and weigh in, and certainly, you know, we are happy to meet with you to discuss that further.

Mr. BANKS. I appreciate it. I hope we can get there before the wheels fall off the bus and correct the problems before it gets to that point.

Ms. HARRIS. Absolutely.

Mr. BANKS. My next question is for anyone who wants to answer it.

The major recent organizational changes in OIT seem to be the creation of the IT Operations and Service Division, which centralized the help desk support and the Enterprise Program Management Office, which is the, quote, "air traffic control tower," if you will, for all of the IT projects.

Are these offices making a positive impact? And, if not, how would you improve it?

Mr. BOWMAN. Every year, we evaluate VA's information security program under FISMA, and we do interact with the ITOPS personnel when we are conducting site visits at 24 VA facilities. We are seeing incremental improvement, some incremental improvements over accountability. We are starting to see roles and responsibilities defined as it relates to IT security, but the improvements have just been marginal at best.

Mr. BANKS. Anybody else? Okay.

Ms. HARRIS. I will say, just in terms of centralization, one of the benefits that we have seen or one of the good things to come out of centralizing IT at VA is in their software license management area.

Previous to VA implementing our recommendations, the management of these licenses were relatively decentralized, and now they actually have a comprehensive inventory of their licenses and they are able to systematically identify the costs and the usage associated with these individual licenses. And so now they are in a better

position to identify cost savings as a result and so that is one of the benefits of this centralization.

I think one of the things that they should be focusing on if they are going to continue this route is, you know, when it comes to IT project management and utilizing and sharing IT best practices in the area of, for example, agile software development, they can harness this type of an approach to ensure that their IT project managers are adequately trained in this area, so that they can have adequate oversight over their contractors who are also utilizing this same software methodology.

Mr. BANKS. I appreciate that. I don't have enough time to ask another question, but I will save more for the second round with that.

I will yield back.

Ms. LEE. Thank you, Mr. Banks.

I would now like to recognize Ms. Brownley from California.

Ms. BROWNLEY. Thank you, Madam Chair, and thank you for holding this hearing that is an important one. And I just want to say that I agree with you wholeheartedly about your disappointment and our disappointment that VA has failed to send a witness here for today's hearing.

You know, Congress has a huge responsibility in terms of oversight and making sure that VA is hitting its benchmarks and it is modernizing its IT systems, especially with large-scale undertakings like the electronic health record—already said, fourth attempt, this was an important one to succeed in—all of the IT systems involved in the implementation of the MISSION Act, just to name a few, it is critically important that we know. So we put a lot of trust in the VA that they are meeting their benchmarks and moving forward in the timeframe that they set out to do, but if they are not here today it is really very hard to have any confidence or trust that VA is doing what they should be doing.

So, I share your concerns and I am disappointed that they are not here.

I wanted to follow up with you, Ms. Harris, on your comment around the CIO and the turnover that it has had. If you could tell us in your opinion, you know, why is this happening? What is causing it? What are the—are there barriers? Is it the job description in and of itself?

Why is it that it is so difficult to have a high-quality leader in this very important position and hold on to that person?

Ms. HARRIS. Well, we have seen a high turnover of CIO leadership across the Federal Government. This isn't a problem that is specific to the VA necessarily, but the actual tenure of less than 2 years makes VA one of the most challenging of the bunch for sure.

I am not quite sure as to why specifically VA can't seem to hold on to a CIO; however, I do commend them for recently making the change of ensuring that the CIO does report directly to the Secretary, because that is an important elevation of the position. I think that that recent change by VA will actually help them have a CIO stay in the position longer, because when that position is elevated then you are going to retain and recruit high-quality CIOs.

And also I think that, you know, when it comes to the CIO position, if VA can have the CIO, Mr. Gfrerer, in this position for about 3 to 5 years, that is when, you know, based on our work, we have seen CIOs become more effective, and especially a large change management program like EHRM, the Electronic Health Records Modernization Program. You are going to want Mr. Gfrerer to be in there at least 3 to 5 years, hopefully longer, 5 to 7 years, where we have actually seen success in public sector organizations.

Ms. BROWNLEY. Thank you. You also mentioned too that it is going to be necessary for the DoD and the VA to iron out its differences and be on the same page in order to properly implement the EHR Modernization. And to me, when I hear that, my sense is that we should stop right now until, you know, we have crossed our Ts and dotted our Is before—that this has to be ironed out first and foremost. It sounds like this is a critical piece, I mean common sense will tell you it is a critical piece, it is the reason why we have been unsuccessful over many, many, many years.

So what are your recommendations in terms of, you know, in our oversight responsibilities how we should proceed?

Ms. HARRIS. Ensuring that VA fully defines the role of the Interagency Program Office with DoD is the most important action that VA can take to ensure that the EHRM program is a success. If they do not fully define that process with DoD, they are going to fail.

Ms. BROWNLEY. Well, that seems abundantly clear.

I know my time is running out, but I just wanted to touch upon the Family Caregiver Program. It is a very important program in terms of its expansion and moving forward and I know, again, the IT systems have really delayed the implementation of that program, and if there were any comments in terms of how that is progressing.

[Pause.]

Ms. BROWNLEY. I yield back my time.

Ms. LEE. Thank you, Ms. Brownley.

I would now like to recognize Mr. Lamb from Pennsylvania.

Mr. LAMB. Thank you very much, Madam Chairwoman.

I want to address a couple of big-picture questions first. And I apologize if this retreads any ground that you covered before I got here, but I just want to open this to all three witnesses.

I see kind of a couple of different ingredients in the recurring problem that we keep having with the Electronic Health Records, with the GI Bill benefits, with some of the issues with disability claims that we have had on the IT side.

There is clearly a management and leadership piece in terms of achieving stable leadership in the CIO position and leadership that is willing to show up for relevant hearings, but then obviously there is an investment component as well. There are many people who feel that the IT infrastructure is outdated.

There is kind of a recurring problem, it seems like, in Federal infrastructure generally where money gets doled out piecemeal over a lot of years in a way that makes it difficult to ever finish the task of a single big investment.

So I guess if you think about those two factors, leadership and money, can you address at all whether one of those is more to

blame for the recurring problems that we keep having or the other, or is it something else entirely?

Mr. BOWMAN. I can certainly talk about our ongoing work with the VA's implementation of FTAR and that relates to the CIO's ability to see IT acquisitions across the enterprise, be involved in the planning, programing, budget, and execution aspect of that. And, although our draft report is under development, we are seeing that the CIO is not actively involved in the planning and budgeting of IT within all the administrations across the enterprise. I think that has a real adverse effect, and then you combine that with the frequent turnover, it is a recipe for disaster.

Mr. LAMB. Ms. Harris, do you have anything to add to that?

Ms. HARRIS. I actually would like to add to what Mr. Bowman is saying about the CIO's absence in the IT budgeting process. Actually within VA, VA does not have any policies associated with the CIO's roles and responsibilities associated with IT strategic planning whatsoever and only a minimal amount of policies in place related to the IT budgeting aspect. And that is a major problem, especially with this frequent turnover of CIOs that we have.

Having codified policies that ensures that the CIO establishes goals for improving agency operations through IT and measuring progress against those goals is absolutely critical. So we have made recommendations in this area and VA should be—we want VA to implement them as soon as possible.

Mr. LAMB. Thank you.

And I think the kind of separate issue that is kind of hanging out there, I think that makes a lot of sense for the year-over-year regular budgeting for IT investments, maintenance, that kind of thing. Obviously, we have the second massive project with the electronic health records.

Given the instability in leadership that we have talked about, again, the unwillingness to show up to a relevant hearing, do you have any suggestions to us as to how we can make sure that this EHR project actually stays on schedule and within budget, or at least that we know when there is a red flag? You know, we don't want to happen on the VA side what happened on the DoD side with this sort of disastrous rollout when it was show time. So, any specific suggestions there?

Ms. HARRIS. Well, the first is defining the role of the IPO and having a single point of accountability, ensuring that DoD and VA have a formalized process for adjudicating those tough issues. That is the first piece.

The second piece is ensuring that VA develops a comprehensive baseline for its EHRM program with a reliable cost estimate and a reliable schedule with performance targets that can be tracked, because what we have seen in these large, major IT programs with VA is that they lack this baseline plan. And so it is really challenging to hold their management accountable in the absence of a plan.

So those are the two key things that VA needs to be set up for success.

Mr. LAMB. Would that differ from the way the DoD did the rollout at the limited number of sites? I mean, I guess, what are you

saying specifically in terms of a performance target, can you give an example?

Ms. HARRIS. Well, I mean, the rollout of sites, I am not saying that that should be necessarily different. I think piloting is certainly the way to go, but having performance targets associated with the system itself, for example, in measuring system defects or measuring customer satisfaction, those are key areas that VA will have to make sure that they have measurable targets in place for.

Mr. LAMB. Thank you.

I yield back.

Ms. LEE. Thank you, Mr. Lamb.

I would now like to recognize Mr. Banks for additional questions.

Mr. BANKS. Thank you very much, Madam Chair.

First of all, Ms. Harris, in your testimony you write that the VA operates 240 information systems. Could you put that into perspective for me a little bit? Is that a lot for an agency the size of the VA? And about how many systems would VA need under optimal conditions?

Ms. HARRIS. Well, VA operates one of the most complex and largest IT networks within the civilian agencies. I mean, you look at their IT budget, it is the third highest behind DHS and HHS. I can't tell you what the right number of systems should be, but considering that 80 percent of their budget goes to maintaining old legacy systems, that is a major problem both from an operational perspective of having to ensure that they have the personnel in place to maintain old code, but also from a cyber security perspective as well, that is a major challenge for them.

So—

Mr. BANKS. Is 240 a lot or that is—because of the complexity of the systems, that is within range of what you would expect?

Ms. HARRIS. I would say that that number is high. And, again, taking a look at where the money is going, since only 20 percent of their money is going towards developing modernized systems, that makes it a problem. So there isn't enough money available to invest into, you know, decreasing that, turning off old legacy systems and investing into new systems.

I can't tell you what the right number would be, but—

Mr. BANKS. Okay, thank you for that. I will move on.

Mr. Bowman, I understand that you manage the VA Cyber Security Audit under the Federal Information Security Modernization Act. In 2015, you found 35 weaknesses; last year, you found 28. That seems like slow progress towards securing veterans' data.

Historically, what has VA done to address the FISMA recommendations and how would you characterize their progress?

Mr. BOWMAN. So when I first came to VA to become the Director back in 2008, there was about 33 outstanding recommendations in connection to the FISMA work. So that if you compare that today from our most recent report, we are now down to 28 recommendations.

Most of the improvement that I have seen VA do is really it is in policy, it is in plans of action and milestones. Incident handling and response has also made an improvement. But as far as making corrections and remediations to address access control issues, con-

figuration management issues, disaster recovery issues, the progress has been just marginal at best. It is—

Mr. BANKS. So what are the barriers that are preventing the VA from—I mean, 35 to 28, that doesn't seem like very good progress to me. What is stopping us from substantially diminishing that number?

Mr. BOWMAN. In my opinion, that VA has to implement a more robust vulnerability management program. They need to be able to identify the vulnerabilities and correct them before we conduct our FISMA audits.

And there are times where VA is seeing these issues at the same time that we are seeing them every year. And so that has to be a more proactive program. They need to be able to patch their systems in a more timely manner. We are finding systems that are outdated with security updates by more than 2 years and these are on the mission-critical systems.

They also need to make IT security a priority and there are years where we just don't feel that they are dedicating the resources to take these issues seriously.

Mr. BANKS. So, a lack of urgency?

Mr. BOWMAN. In my opinion, yes.

Mr. BANKS. Okay. Of the 28 recommendations last year, the VA didn't concur with three of them, claiming that they had already been resolved. Can you explain these recommendations and whether or not you agree with the VA's position?

Mr. BOWMAN. Well, part of it was is that we sat with VA several times, we asked for them to provide us supporting documentation, so that we could conclude whether or not the corrective action plans had been remediated. VA did not provide them to us, nor were we able to perform any subsequent testing, and for that reason those recommendations remain.

Now, going forward, we are going to put efforts to see whether or not those corrective action plans are effectively mitigating the vulnerabilities. It just remains to be seen right now, but I don't feel VA made a concerted effort to give us the information we were asking for.

Mr. BANKS. All right, let me get one more question in really quick, continuing on the same subject. What are the VA's most significant risks from its many systems that are connected with external organizations?

Mr. BOWMAN. I think it is very important you have got to monitor all system interconnections on the VA networks. They have got hundreds of business partners, they have got numerous connections in and out of the network. VA doesn't monitor all those systems.

Now, going forward, there is only maybe about five or six that aren't monitored, which is better than how they were doing 4 or 5 years ago, but you really shouldn't have any interconnections that weren't monitored, because your partners, their security posture may be far worse than VA. They could be a vector right into your network and, without monitoring it, VA doesn't know whether or not its systems are infiltrated.

Mr. BANKS. Thank you. My time has expired.

Ms. LEE. Thank you, Mr. Banks.

I want to talk about, you know, successful IT programs require that agencies know exactly what they are building or buying, who the users are and what they are actually going to need. This is requirements development and it takes a lot of legwork by the agency to research and talk to stakeholders, and it is also a place where many agencies under time and money constraints tend to fall short.

Mr. Arronte or Ms. Harris, either one of you, what are some of the best practices that the GAO and OIG have identified regarding requirements development and recommendations?

Ms. HARRIS. One of the most critical success factors in delivering major IT programs is, as you mentioned, requirements development and management, ensuring that the program is adequately involving the end users in the development of those requirements. And then from there prioritizing requirements, because as if, for example, funding becomes unstable or gets cut, you are going to want to be able to very quickly, you know, de-scope the program as necessary.

And so those are the two critical success factors that we have found regarding requirements in delivering IT systems.

Mr. BOWMAN. I definitely agree that agile software development practices. The sooner you get the end users involved in developing the requirements and testing it and on the rollout, you are more likely to hit your targets. But I think it is also important that VA stabilize their functionality requirements. A lot of times in these projects they will go in with a general idea of what they want and, as they start developing a road plan, they realize that they need a lot more functionality to achieve end user goals and to meet the goals of the project. So, without stabilizing that, you are not going to hit your schedule, you are not going to hit your cost goals, and then the system will not perform as intended.

Ms. LEE. Thank you. Mr. Arronte, the OIG reviewed the issue of unwarranted medical examinations for disability benefits and found that the VBA needed to take steps to prioritize the design and implementation of system automation reasonably designed to minimize unwarranted reexaminations. The VBA then concurred with the recommendation, but the OIG Web site says it was not implemented because, quote, "the recommendation was unable to be satisfactorily addressed despite significant efforts due to the lack of resources or other reasons."

Could you elaborate on that?

Mr. ARRONTE. Yes, and this was kind of a surprise to us. Typically, we meet with the Department and we discuss our recommendations. They came back; they felt that the recommendation was a good recommendation that they wanted to implement. And then, as they started moving along the course to implement, OI&T came and told them, well, we might be able to do this, but it is going to be 18 to 24 months before we can do this. And when we make our recommendations, we try to gear our recommendations to be implementable within a year. So, once VBA leadership was notified that this was not going to happen in a year, they came back to us and said, look, we are not going to be able to do this; not that we don't agree with it and not that we don't want it, but OI&T is telling us 18 to 24 months.

Ms. LEE. So there was no way to sort of define what could be accomplished within a year?

Mr. ARRONTE. No. And OI&T, the way they prioritize what is important is—I can speak from VBA, VBA senior leadership has conveyed to me that it is unclear to them how OI&T prioritizes work across the Department.

Ms. LEE. Okay, that is surprising.

Ms. Harris, one more question. I have just a little bit of time. One of the issues that the GAO cited with regards to the Forever GI Bill implementation was that the VBA Education Service and the Office of Information and Technology could not agree on what a working solution was.

You know, we have talked about having a single point of accountability can be helpful to prevent this type of disagreement, but what other types of mechanisms can an agency have in place that would help keep the project's scope on track?

Ms. HARRIS. Well, certainly having strong leadership in place is absolutely vital and ensuring that program staff have the necessary knowledge and skills from an IT management and contractor oversight perspective. Those are two major areas that are common to successfully delivering an IT system.

Ms. HARRIS. Thank you.

I now yield to Mr. Banks.

Mr. BANKS. Thank you, Madam Chair.

Mr. Arronte or Mr. Bowman, the VA also undergoes a financial statement audit every year, which includes IT systems and cyber security. I understand there are many material weaknesses in that audit as well. What actions should VA take to correct the material weaknesses?

Mr. ARRONTE. So Mr. Bowman is going to speak specifically to some of the IT challenges. We do have one that is directly related to information technology and it is ensuring effective information security program and system controls. And one of the things that we see—and we have talked about budget and management and which one is more or less important—with these security controls and the CIO not being part of the budget process, what we find is medical centers are purchasing IT equipment under their own budget, and then what happens is the CIO is unaware that this equipment has been purchased, so the CIO is not—there is no process to ensure that the security of this equipment is in place because the CIO was unaware of it.

Mr. BOWMAN. Related to IT, even though that my focus is of FISMA, part of that focus is to evaluate the IT controls in connection with the consolidated financial statement audit as well, and so what we see in FISMA is basically duplicate issues that we find for the consolidated financial statement.

So the real issues, the way for VA to remediate the material weakness and get it downgraded to a significant deficiency is we have got to see password controls consistently implemented across all systems. And we still see passwords with the same user name and passwords sometimes 2 and 3 years running, we have got default passwords. And, you know, when you are briefing the VA Secretary and we start explaining that, it is really uncomfortable, because that seems like very low-hanging fruit and why is that a dis-

cussion point every year when we brief out on the financial statement. So that is first and foremost.

The other thing—

Mr. BANKS. You brief that over and over again, but little to no progress in addressing it?

Mr. BOWMAN. It certainly gets a lot of air time at the meeting and, you know, there is a lot of focus that says, well, we are going to get rid of this next year. Either our testing methods are very good or just VA is lax, it is hard to tell. Sometimes we just go back and test the same systems and we will find those same user accounts with unchanged passwords.

But the other thing is, is VA has legacy systems that are no longer supported by the vendor, so they can't update those systems for, you know, hot fixes and security patches to address emerging IT security issues.

And so, unless you resolve those, the material weakness will remain.

Mr. BANKS. Unbelievable, but let's move on.

Mr. Arronte, in your testimony you cite the VA IT budget proposal as $4.3 billion. Does that include all IT spending?

Mr. ARRONTE. No, sir, it does not. And, as I alluded to earlier, what happens is VHA has a specific line item for the purchases of IT equipment, which I was in a meeting and we asked the CFO at the time, why is there a specific line item for the hospitals or the VA MCs or the VISNs to purchase IT equipment without going through the CIO? And what we were told was it takes the CIO's office too long to approve equipment that we need now.

Mr. BANKS. So let me ask you, what are the practical consequences of having IT activities that the Chief Information Officer isn't aware of?

Mr. ARRONTE. So, one, cost overruns; two, duplication of IT acquisition equipment; and, third, not being able to—because you are unaware of this equipment, you can't place security on it and you can't track it, and then it becomes an inventory issue as well.

Mr. BANKS. That is startling and troubling, and, with that, I will yield back.

Ms. LEE. I am going to continue on this with respect to the electronic health records revamp that we are doing in terms of the acquisition process.

Do you have recommendations? I mean, we have the $10 billion contract with Cerner and then the $6 billion that the VA needs to use for the infrastructure and the equipment. Are there recommendations you have to make sure that process is as successful as possible?

Mr. ARRONTE. So we have not done any formal work with EHR. We have staff that attend clinical council meetings to monitor the progress. Right now we understand that there are discussions between VA and DoD on medical coding. Until some of that is resolved, I am not sure what our role is going to be with the limited resources we have. But I think a good answer is, look at the past practices, look at the past—like Mr. Banks indicated, 33 recommendations, 28 recommendations, they can't get security on equipment right.

I think VA risks—this is a behavior for VA, and I think what is the potential risk for EHR is these types of behaviors will roll over into this initiative, and that is what we are looking at right now.

Ms. LEE. Okay.

Ms. HARRIS. Madam Chair, we intend to initiate work on the EHR program very soon. We have ongoing work at VistA, as well as ongoing work on the DoD side, the MHS Genesis program. So we have not made specific recommendations related to the EHR acquisition itself, but we do have the one outstanding recommendation to define the role of the Interagency Program Office.

And again, as I mentioned earlier, if that process hasn't been formalized, whatever VA does on the acquisition, I mean, it is ultimately going to fail in terms of the interoperability with DoD.

Ms. LEE. Thank you.

Ms. HARRIS. So they have to get that right.

Ms. LEE. Thank you.

Well, this has been somewhat depressing, but also a helpful discussion. And we certainly look forward to working with the VA to ensure that we help overcome these deficiencies, because ultimately making sure that we are successful means better care for our veterans, which is ultimately the goal for all of us.

So I look forward to continuing as the Subcommittee moves forward with oversight of technology and modernization at the VA.

I would like to thank all of our witnesses for your attendance and your testimony, and your patience in answering these questions.

And all Members will have 5 legislative days to revise and extend their remarks and include extraneous material.

And this hearing has now been adjourned. Thank you.

[Whereupon, at 11:18 a.m., the Subcommittee was adjourned.]

A P P E N D I X

Prepared Statement of Mark Takano, Chairman Full Committee

Good Morning. This hearing will come to order.

This is the first hearing of the 116th Congress by the Subcommittee on Technology Modernization. This Subcommittee was created last year because this Committee recognized that all aspects of implementing technology at the Department of Veterans Affairs needs sustained attention and oversight.

I am pleased that the work that was begun last year will continue and I am honored to be a part of the effort. I look forward to working with my colleague, Ranking Member Banks, and the other members of the Subcommittee on this important mandate.

VA has many technology modernization projects underway, from the Electronic Health Record Modernization, the Financial Management Business Transformation, and efforts to update its supply chain system. Congress has also given VA several critical programs to implement, including the MISSION Act and the Forever GI Bill. These programs will need to have strong technology systems that support the successful delivery of healthcare and benefits to our veterans.

The Subcommittee will engage in oversight of each of these programs over the next several months. However, I thought it would be helpful to begin the Subcommittee's work with an assessment of the office within VA that bears much of the responsibility for implementing the technology that will support these critical programs.

The Office of Information and Technology (OI&T) is responsible for all aspects of technology modernization at VA, including acquisition, development, and implementation. OI&T is also responsible for making sure that VA's critical systems are secure, and that veterans' personal data is protected.

It is clear that OI&T has struggled in its mission.

Many decades of oversight work by the Government Accountability Office and the Office of Inspector General have found and documented systemic leadership and management challenges at OI&T. Progress at solving these problems has been halting.

Today, I would like to explore the root causes of these challenges and to identify the barriers to improvement. And if OI&T has made progress I would like to explore that as well, so that we can determine how successful results can be replicated.

One of the major problems at OI&T has been high turnover in leadership. VA has had five chief information officers in four years. I am glad that a confirmed leader is now in place and I wish Mr. Gfrerer success in his position and I hope that he is able to implement some of the critical change that is needed at OI&T.

However, you will note that we have an empty chair at the table where the Office of Information and Technology should be represented. The Subcommittee invited Mr. Gfrerer to the hearing today, but the VA declined because he is testifying before the Full Committee this afternoon. That is somewhat understandable, and we told VA that we would accept a deputy for testimony today. We won't stand on ceremony in this Subcommittee. We want to engage with knowledgeable management and staff - no matter their title - to better understand these challenges and to figure out solutions. Unfortunately, VA refused the Subcommittee's request.

I hope we will hear from OI&T at a Subcommittee hearing in the near future, because if we want VA to be able to successfully deliver healthcare and benefits to our Veterans, OI&T has to be an effective part of that effort. There is no doubt that we want OI&T to succeed at its mission, because its success means that veterans get the highest level of care and reliable access to the benefits they have earned.

I am pleased to have members of our oversight community here today to help the Subcommittee further its own oversight of technology at VA. I look forward to testimony from GAO and the OIG and engaging in discussion with them now and going forward.

Thank you.

Prepared Statement of Carol C. Harris

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

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 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 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.

---

[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).

[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).

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.

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

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

[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.

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 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.

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

[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).

[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.

[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.

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. [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;
- 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,

---

[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).

[19] The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113–283, Dec. 20, 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).

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.

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.

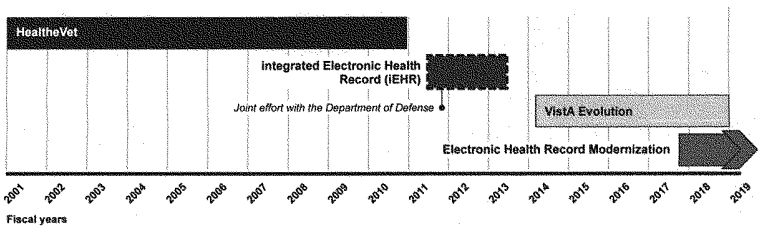
VA Has Made Limited Progress toward Addressing IT System Modernization Challenges

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.

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.

---

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

[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).

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 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. Accord-

[24] GAO 08 805.
[25] FAR, 48 C.F.R. § 6.302–7.

ingly, 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 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.

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 pro-

---

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

[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).

[29] GAO 14 675.

gram 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.

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 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 depart-

[30] GAO 15 582.
[31] GAO 16 494, GAO 16 469, GAO 18 148, GAO 18 264, GAO 18 93.

ment 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 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 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

---

[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.

[34] GAO 18 264.

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

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.

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 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

---

[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.

[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.

[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.

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 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 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.

---

[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).

[43] GAO 16 501.

[44] GAO 19 144.

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.

GAO HIGHLIGHTS

Why GAO Did This Study

The use of IT is crucial to helping VA effectively serve the nation's veterans. Each year the department spends billions of dollars on its information systems and assets. However, VA has experienced challenges in managing its IT programs, raising questions about its ability to deliver intended outcomes needed to help advance the department's mission. To improve federal agencies' IT acquisitions, in December 2014 Congress enacted FITARA. GAO has previously reported on IT management challenges at VA, as well as its progress in implementing FITARA and cybersecurity requirements.

GAO was asked to summarize key results and recommendations from its work at VA that examined systems modernization efforts, FITARA implementation, and cybersecurity efforts.

To do so, GAO reviewed its recently issued reports and incorporated information on the department's actions in response to GAO's recommendations.

What GAO Recommends

GAO has made numerous recent recommendations to VA aimed at improving the department's IT management. VA has generally agreed with the recommendations and has taken steps to address them; however, the department has fully implemented less than half of them. Fully implementing all of GAO's recommendations would help VA ensure that its IT effectively supports the department's mission.

View GAO–19–476T. 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 made limited progress toward addressing information technology (IT) system modernization challenges.

- From 2001 through 2018, VA pursued three efforts to modernize its health information system-the Veterans Health Information Systems and Technology Architecture (VistA). However, these efforts experienced high costs, challenges to ensuring interoperability of health data, and ultimately did not result in a modernized VistA. Regarding the department's fourth and most recent effort, the Electronic Health Record Modernization, GAO recently reported that the governance plan for this program was not yet defined. VA has not fully implemented GAO's recommendation calling for the department to define the role of a key office in the governance plans.
- The Family Caregiver Program, which was established to support family caregivers of seriously injured post-9/11 veterans, has not been supported by an effective IT system. Specifically, GAO reported that, due to limitations with the system, the program office did not have ready access to the types of workload data that would allow it to routinely monitor workload problems created by the program. GAO recommended that VA expedite the process for identifying and implementing an IT system. Although the department concurred with the recommendation, VA has not yet fully addressed it.

- VA had developed the Veterans Benefits Management System-its system that is used for processing disability benefit claims; however, the system did not fully support disability and pension claims, as well as appeals processing. GAO made five recommendations for VA to improve its efforts to effectively complete the development and implementation of the system. The department concurred with the recommendations but has implemented only one thus far.

VA has demonstrated uneven progress toward fully implementing GAO's recommendations related to key Federal Information Technology Acquisition Reform Act (FITARA) provisions. Specifically, VA has implemented all six recommendations in response to GAO's 2014 report on managing software licenses, leading to, among other things, savings of about $65 million over 3 years. However, the department has not fully addressed two recommendations from GAO's 2016 report on managing the risks of major IT investments. Further, the department has not implemented (1) two of four recommendations related to its effort to consolidate data centers and (2) GAO's four recommendations to increase the authority of its Chief Information Officer.

VA's management of cybersecurity has also lacked key elements. For example, GAO reported in May 2016 that VA had established numerous security controls, but had not effectively implemented key elements of its information security program. In addition, as GAO reported in March 2019, the department had not accurately categorized positions to effectively identify critical staffing needs for its cybersecurity workforce. VA has implemented three of six cybersecurity-related recommendations from these two reports.

Brent Arronte

Madam Chair, Ranking Member Banks, and members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG's) oversight of VA's Office of Information and Technology (OIT). Our statement will focus on the effectiveness of VA's information security program, the progress made, and challenges VA continues to face in developing the information technology (IT) systems needed to effectively carry out their mission. We base our conclusions on OIG reports on VA's information security program and our ongoing oversight of IT systems development and management. I am accompanied by Mr. Michael Bowman, Director of the OIG's Information Technology and Security Audits Division.

BACKGROUND

Since 2000, the OIG has identified information management as a major management challenge because VA has a history of not properly planning and managing its critical IT investments. [1]

For fiscal year (FY) 2020, VA requested a total IT investment of $4.3 billion to fund information system security, system development initiatives, and system operations and maintenance.

IT systems and networks are critical to VA in carrying out its mission of providing medical care and a range of benefits and services to veterans and their families. Ensuring the secure operation of these systems and networks is essential given the wide availability and effectiveness of internet-based hacking tools. Lack of proper safeguards renders these systems and networks vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other VA systems. VA has previously reported security incidents in which sensitive information, including personally identifiable information, has been lost or stolen, potentially exposing millions of veterans and their families to the loss of privacy, identity theft, and other financial crimes. [2]

MAJOR CHALLENGES FACING OIT

OIG audits have consistently shown that IT systems development is a challenge for VA. Projects are susceptible to cost overruns, schedule slippages, performance problems, and in some cases, complete failure. The OIG has identified significant control deficiencies in the IT areas of security, project management, and system development that are discussed in more detail below. By continuing to identify deficiencies, make recommendations, and oversee implementation plans, the OIG's goal is to help VA:

[1] Office of Inspector General 2018 Major Management Challenges, November 2018.
[2] Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans, July 11, 2006.

- Strengthen areas of IT security weakness to effectively safeguard veterans' personal information and benefits.
- Properly plan and manage IT projects to deliver a timely and cost-effective product that adequately satisfies the needs of VA staff.

IT Security

VA's fundamental mission of providing benefits and services to veterans is dependent on deploying secure IT systems and networks. VA's information security program and its practices must be designed to protect the confidentiality, integrity, and availability of VA systems and data.

Federal Information Security Management Act of 2002 Audit. The Federal Information Security Management Act of 2002 (FISMA) requires that agencies and their affiliates, such as government contractors, develop, document, and implement an organization-wide security program for their systems and data. In FY 2018, the OIG's contractors completed audits to review the extent to which VA had appropriate IT safeguards in place.[3] The audit concluded that VA has made progress producing, documenting, and distributing policies and procedures as part of its program. However, VA continues to face hurdles implementing components of its agencywide information security risk management program to meet FISMA requirements.

Significant deficiencies persist related to system access controls, system configuration management controls, system hardware and software change management controls, as well as system disaster recovery practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction. To address these deficiencies, VA must prioritize remediation of these security weaknesses, as ongoing delays in implementing effective corrective actions may contribute to the continued reporting of an information technology material weakness in VA's financial statements. The FY 2018 FISMA report contained 28 recommendations to the Assistant Secretary for Information and Technology for improving VA's information security program. These recommendations focused on improving the following security domains:

- System access controls to include password standards and user account reviews
- System configuration management controls to include timely system security updates
- Information security management controls such as consistently updating Plans of Action and Milestones and System Security Plans
- System disaster recovery practices for critical systems

The Principal Deputy Assistant Secretary for Information and Technology concurred with 25 of 28 recommendations and provided acceptable action plans. While the Principal Deputy Assistant Secretary did not concur with three recommendations, the OIG believes these recommendations warrant further attention from VA and will follow up on these issues during the FY 2019 FISMA audit.

Use of Unauthorized Databases. The OIG conducted a review in response to anonymously reported allegations that the VA Long Beach Healthcare System (the system) in California was maintaining an unauthorized Microsoft Access database, the unauthorized database hosted Sensitive Personal Information (SPI), and all of the Veterans Health Administration's 24 Spinal Cord Injury Centers had access to the database through a Microsoft SharePoint intranet portal.[4] The complaint also stated that unsecured veteran SPI was stored on a server outside of VA's protected network environment. The OIG substantiated the allegation related to the unauthorized database at the system. Consistent with the allegation, the OIG found multiple instances of databases that hosted SPI in violation of VA policy. The OIG also substantiated that veteran SPI was hosted on an external server, located at the University of Southern California, without a formal Data Use Agreement authorizing such activity. In addition, the review team noted this server could be accessed from the internet using default logon credentials. The OIG recommended the Under Secretary for Health ensure that the Spinal Cord Injury and Disorders program staff comply with VA's Privacy Program and information security requirements for all sensitive veteran data collected, the Executive Director for the National Spinal Cord Injury Program Office discontinue storing SPI in unauthorized Microsoft Access databases, and the Acting Assistant Secretary for Information and Technology ensure that Field Security Services and VA's Privacy Service implement improved procedures to identify unauthorized uses of SPI and take appropriate corrective ac-

[3] Federal Information Security Modernization Act Audit for Fiscal Year 2018, March 12, 2019.
[4] Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System, March 28, 2018.

tions. The three responsible offices concurred with the recommendations. VA provided corrective action plans that were responsive to the recommendations. Based upon our review of VA's corrective actions, the OIG has closed all report recommendations.

IT Project Management and System Development

VA must continue to invest in and improve IT project management and system development so that future initiatives and major projects can experience more efficient and seamless rollouts. To the extent that VA does not properly plan and manage these IT investments, they risk overrunning projected costs and delivering products that do not consistently align with user requirements.

Real Time Location System Review. The OIG conducted a review based on concerns of contract mismanagement involving the development and implementation of the Real Time Location System (RTLS), a product that uses multiple technologies for locating and tracking medical equipment.[5] At the time of the review, VA was in the process of deploying RTLS at all medical facilities nationwide. The team determined that management failed to comply with VA policy and guidance when it deployed RTLS assets without appropriate project oversight. Specifically, the OIG concluded the RTLS Project Management Office (PMO) did not follow guidance to use an incremental project management approach during the acquisition and deployment of RTLS assets to compensate for numerous known project management risks. Consequently, the RTLS PMO did not ensure the vendor could meet contracted functionality requirements on the initial $7.5 million task order, such as accurate asset tracking, before ultimately committing a total of $431 million to the same vendor for further RTLS deployments. The OIG reported that management failed to provide effective oversight of the RTLS project from acquisition through development and implementation to ensure the product was successfully deployed.

The OIG also reported that VA deployed RTLS assets without meeting VA's information security requirements. Specifically, RTLS assets were deployed without the appropriate system authorizations needed to connect such devices to VA's network. This inadequate oversight of RTLS risk management activities left VA mission-critical systems and data susceptible to unauthorized access, loss, or disclosure. Consequently, VA's internal network faced unnecessary risks resulting from untested RTLS system security controls. In response to the OIG's findings, the Acting Assistant Secretary reported that OIT will conduct risk assessments prior to future deployments and will enforce the use of incremental project management to ensure an adequate return on investment. VA provided corrective action plans that were responsive to the OIG's recommendations. Based upon its review of VA's corrective actions, the OIG has closed all report recommendations.

Data Center Consolidation. The OIG conducted an audit to determine whether VA met the data center requirements of the Federal Information Technology Acquisition Reform Act (FITARA).[6] Specifically, the OIG assessed whether VA accurately identified and reported data center inventories, achieved cost savings, and met the Office of Management and Budget's Data Center Optimization Initiative (DCOI) targets for data centers at existing VA facilities. The OIG found that VA faced several challenges in identifying data centers VA-wide, establishing a sufficient plan to achieve cost savings and avoidance targets, and meeting optimization metrics and closures. The OIG determined that all VA data centers were not accurately reported to OMB and VA's strategic plan was inconsistent with DCOI requirements due to missing and incomplete information. Without an accurate inventory of data centers or a credible plan to increase operational efficiency and achieve cost savings, VA will continue to operate in an IT environment that is at greater risk for duplication and waste. The OIG made five recommendations, and the Principal Deputy Assistant Secretary for IT concurred and has provided an acceptable action plan for four of the five recommendations.

Veterans Benefits Management System. A key part of the Veterans Benefits Administration's (VBA's) modernization efforts involved replacing its paper-based claims process with an automated solution that integrates commercial and government off-the-shelf web-based technology and improved business practices. VBA and OIT jointly developed the Veterans Benefits Management System (VBMS).

---

[5] Review of Alleged Mismanagement of VA's Real Time Location System Project, December 19, 2017.

[6] Lost Opportunities for Efficiencies and Savings During Data Center Consolidation, January 30, 2019.

- In 2015, the OIG reviewed how effectively VA was managing the cost, performance, and schedule of VBMS development.[7] While the OIG found that VA stayed on schedule in deploying planned VBMS functionality to all VA regional offices, VBMS costs increased significantly, more than doubling from about $579.2 million to approximately $1.3 billion from 2009 to 2015. The increases were due to inadequate cost control, unplanned changes in system and business requirements, and inefficient contracting practices. As a result, VA could not ensure an effective return on its investment and total actual system development costs remained unknown. The OIG recommended the Executive in Charge for OIT, in conjunction with the Under Secretary for Benefits, define and stabilize system and business requirements, address system performance problems, deploy required functionality to process claims end-to-end, and institute metrics needed to identify and ensure progress toward meeting stated goals. While this report is from 2015, it highlights issues with IT project management that VBA continues to face.

In recent OIG reports on the processing of disability claims, the OIG found that VBMS functionality issues have contributed to concerns related to the processing of benefits.

- In a review of whether VBA staff assigned correct effective dates on claims for compensation benefits with an intent to file, the OIG determined that inaccurate dates for these claims partially occurred because VBMS lacked the needed functionality to assist rating personnel when assigning effective dates for benefits based on intent to file claims.[8] The intent to file allows claimants the opportunity to provide minimal information related to the benefit sought and gives them up to one year to submit a complete claim. The OIG found that VBA assigned incorrect effective dates for approximately 17 percent of compensation benefits with receipt of the intent to file from claimants. VBA concurred with the OIG's recommendation related to functionality and indicated a correction is due in late 2019.
- In a review to determine whether VBA employees required disabled veterans to submit to unwarranted medical reexaminations, the OIG also found VBMS functionality issues.[9] The OIG determined that many unwarranted medical reexaminations occurred because VBMS did not have the functionality to prevent the scheduling of reexaminations in cases that met the exemption criteria. While reexaminations are important in certain situations to ensure taxpayer dollars are appropriately spent, unwarranted reexaminations cause undue hardship for veterans. They also generate excessive work, resulting in significant costs and the diversion of VA personnel from veteran care and services. VBA concurred with the OIG's recommendation and stated that VBA and OIT are in the process of developing automated examination request requirements and anticipate full functionality in FY 2019, pending prioritization and approval of new development efforts.

Forever GI Bill. In March 2019, the OIG released an issue statement in response to allegations that VA planned to withhold retroactive payments for missed or underpaid monthly housing stipends that it failed to pay students under the Harry W. Colmery Veterans Education Assistance Act, also known as the Forever GI Bill.[10] Given the impact of delayed or incorrect payments on veterans and congressional concerns, the OIG examined VA's timeline of early implementation actions and the impediments to meeting Forever GI Bill mandates. The OIG found that VBA failed to modify their electronic systems, such as the Long-Term Solution application, by the required implementation date to make accurate housing allowance payments under sections 107 and 501 of the law. VA also lacked an accountable official to oversee the project during most of the effort. Ineffective program management resulted in unclear communication of implementation progress and inadequately defined expectations, roles, and responsibilities of the various VA business lines and contractors involved.[11] The OIG also found that approximately 10 months passed from the time Congress enacted the Forever GI Bill until VA received the initial software development release and began testing the system modi-

[7] Follow-up Review of VA's Veterans Benefits Management System, September 14, 2015.
[8] Processing Inaccuracies Involving Veterans' Intent to File Submissions for Benefits, August 21, 2018.
[9] Unwarranted Medical Reexaminations for Disability Benefits, July 17, 2018.
[10] Forever GI Bill: Early Implementation Challenges, March 20, 2019.
[11] The VA business lines and contractors involved include OIT, VBA Education Service, VBA Office of Business Process Integration, Booz Allen Hamilton, and VA leaders.

fications to VA's Long-Term Solution application in order to address sections 107 and 501 of the law.

ONGOING OVERSIGHT INITIATIVES

OIG engagements that are planned or underway will provide additional oversight of VA's IT management and IT security programs.

The FY 2019 FISMA audit will determine the extent to which VA's information security program and practices comply with FISMA requirements. This annual audit will evaluate selected management, technical, and operational controls supporting 49 selected major applications and general support systems hosted at 25 VA facilities, including VA's four major data centers. As previously discussed, in 2018 the OIG reported that VA has made progress developing, documenting, and distributing policies and procedures as part of its program. However, VA still faces challenges implementing components of its agency-wide information security risk management program to meet FISMA requirements. The OIG's 2019 audit will determine whether VA's improvement efforts are adequate to remove the IT material weakness from the OIG's report on VA's financial statements.

The OIG is also conducting an audit to determine whether VA has implemented key elements of FITARA Section 831, Chief Information Officer Authority Enhancements. Specifically, this audit will evaluate the extent to which the Chief Information Officer met requirements to: (1) review and approve all IT asset and service acquisitions across the VA enterprise; and (2) participate in VA's IT planning, programming, budgeting, and execution, including governance, oversight, and reporting.

The OIG is monitoring many facets of VA's Electronic Health Record Modernization project, implementation of the MISSION Act, and other IT initiatives. As VA moves forward with these projects, the OIG will track the progress made and determine the most efficient and useful ways to provide oversight of VA's ongoing work.

CONCLUSION

Advances in IT enable VA to more effectively deliver benefits and services to our nation's veterans and their families. It is imperative that VA maintain secure systems and properly develop new systems. Until a proven process is in place to ensure control across the enterprise, the IT material weakness will remain and VA's mission-critical systems and sensitive veterans' data will be at risk of attack or compromise. While VA has made recent improvements in information management, more work remains to be done and VA must continue to address OIG recommendations related to the security and development of IT systems. The OIG will continue to conduct oversight of OIT initiatives and major projects to ensure they are secured, developed, and managed appropriately.

Madam Chair, this concludes my statement. We would be happy to answer any questions you or other members of the Subcommittee may have.