REBOOT: EXAMINING THE U.S. DEPARTMENT OF VETERANS AFFAIRS INFORMATION TECHNOLOGY STRATEGY FOR THE 21ST CENTURY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

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

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 11, 2011

Serial No. 112–12

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE
67–187 WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON VETERANS' AFFAIRS

JEFF MILLER, Florida, *Chairman*

CLIFF STEARNS, Florida
DOUG LAMBORN, Colorado
GUS M. BILIRAKIS, Florida
DAVID P. ROE, Tennessee
MARLIN A. STUTZMAN, Indiana
BILL FLORES, Texas
BILL JOHNSON, Ohio
JEFF DENHAM, California
JON RUNYAN, New Jersey
DAN BENISHEK, Michigan
ANN MARIE BUERKLE, New York
TIM HUELSKAMP, Kansas
Vacancy
Vacancy

BOB FILNER, California, *Ranking*
CORRINE BROWN, Florida
SILVESTRE REYES, Texas
MICHAEL H. MICHAUD, Maine
LINDA T. SÁNCHEZ, California
BRUCE L. BRALEY, Iowa
JERRY MCNERNEY, California
JOE DONNELLY, Indiana
TIMOTHY J. WALZ, Minnesota
JOHN BARROW, Georgia
RUSS CARNAHAN, Missouri

HELEN W. TOLAR, *Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

BILL JOHNSON, Ohio, *Chairman*

CLIFF STEARNS, Florida
DOUG LAMBORN, Colorado
DAVID P. ROE, Tennessee
DAN BENISHEK, Michigan
BILL FLORES, Texas

JOE DONNELLY, Indiana, *Ranking*
JERRY MCNERNEY, California
JOHN BARROW, Georgia
BOB FILNER, California

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

May 11, 2011

REBOOT: EXAMINING THE U.S. DEPARTMENT OF VETERANS AFFAIRS INFORMATION TECHNOLOGY STRATEGY FOR THE 21ST CENTURY

WEDNESDAY, May 11, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:00 a.m., in Room 334, Cannon House Office Building, Hon. Bill Johnson [Chairman of the Subcommittee] presiding.

Present: Representatives Johnson, Roe, Donnelly, and Barrow.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Mr. JOHNSON. Good morning. This hearing will come to order.

I want to welcome everyone to today's hearing entitled, "Reboot: Examining VA's IT Strategy for the 21st Century."

With an information and technology (IT) budget exceeding $3 billion annually, it is reasonable for the American taxpayer to expect the Office of Information and Technology (OI&T) at the U.S. Department of Veterans Affairs (VA) to effectively utilize available technology and provide the highest quality support in the Department's delivery of health care and benefits to our Nation's veterans.

As we will hear from the witnesses on both panels today, billions of dollars have been spent on IT at the VA. However, veterans, the taxpayers, and Members of this Committee are left to wonder what has resulted from these expenditures.

Have improvements been made? Certainly they have. Are the improvements and advancements in VA IT over the last 10 years on par with the amount of time and taxpayer dollars put into the effort? Certainly not.

The witnesses on today's second panel will help illuminate the magnitude of the money spent on IT over time. To name just a few, $127 million over 9 years on an outpatient scheduling system with none of the planned improvements in place; suspension of the Strategic Asset Management or SAM Program after failing to meet yet another milestone; and $70 million in an overrun on a WiFi installation contract.

I also remain concerned that, as with past contracts and efforts, VA is not thoroughly vetting cost and risk analysis before undertaking new large IT projects.

While VA continues to push forward on cloud computing, its own administration has not fully established the Federal guidelines for information security in cloud computing.

In a health care environment such as VA's, I know that I would not want my personally identifiable information floating around in the cloud especially given a track record of data breaches that is less than stellar.

We once again notice a history of poor acquisition and contract management at VA, a theme this Subcommittee is familiar with. Given the frequency of problems in IT contracts, we know there must be a significant degree of inexperience among the contracting staff, but we are also left to wonder whether supervisors at OI&T either do not know or do not care about these shortcomings.

When IT needs are not clearly defined at the beginning of the process, it leads to cost increases and time delays down the road. With an IT staff of over 7,000, I find it difficult to believe that knowledgeable IT professionals are not helping to create a well-defined request for proposal, a key element of a viable contract.

When these contracts constantly have to be modified, it results in greater cost to the taxpayer and a delay of improved services to our veterans.

A crucial area for VA IT to meet expectations is the establishment of the joint electronic health record or EHR with the U.S. Department of Defense (DoD). Yet, another overdue item for our active-duty servicemembers and our veterans, the EHR has been pursued separately by the two departments. The result is billions of dollars spent, much of it duplicative, and no joint EHR.

While I commend the secretaries of both departments for finally committing this spring to cooperatively pursue this endeavor, I have lingering concerns that mistakes made in previous IT contracts could be repeated.

For example, after releasing a final Request for Proposal (RFP) on an open-source custodial agent at the end of last month, VA is only allowing a 3-week turnaround for proposals to be submitted at the end of this week.

It is not rocket science. The capabilities to do what needs to be done already exist. Hundreds of millions of dollars could have been saved in previous years by simply having a robust IT architecture and strategy in place.

When needs are clearly defined, protect veterans' information, establish an electronic health record in conjunction with DoD, and implement stringent oversight of these and all undertakings in the Office of Information and Technology, everybody benefits, the taxpayer and the veterans.

I fully understand the challenges of managing information technology in a large organization because I have done so. What I do not understand is why it has taken so long to get only so far at VA.

The American people are watching and expect VA to take care of our veterans as promised.

Again, I appreciate everyone's attendance at today's hearing and I now yield to the Ranking Member for his opening statement.

Mr. Donnelly.

[The prepared statement of Chairman Johnson appears on p. 23]

OPENING STATEMENT OF HON. JOE DONNELLY

Mr. DONNELLY. Thank you, Mr. Chairman.

Secretary Shinseki has often stated the need to transform the VA to meet the changing needs of our warriors. A perfect example of this was when the VA found themselves having to process education claims manually due to the Legacy System being unable to process these claims after the passage of the recent historic GI Bill legislation.

For this reason, I find it important and critical that the VA maintains an updated IT system that proves to be reliable and can be manipulated as new software is incorporated through the years ahead.

The VA has decided that using an open-source model will provide a better outcome with lower risks and lower cost. Their cooperation with the DoD on using open source is encouraging, in part because this cooperation is essential. There is a critical need to develop an interoperable electronic health record system and because DoD has relied on open source in the past.

Although there are multiple concerns on both sides of the aisle, the VA has reassured us that open source provides several benefits. But along with those benefits, making sure that veterans' personal information remains secure is critical.

I also understand that contract management and weaknesses have overshadowed VA's efforts to keep up with the VA's IT infrastructure. Cost overruns, contract weaknesses, and unmet project time frames are just a few examples of the implications that can occur if there are no firm requirements in contracts. Such was the case with the WiFi awarded contract to Catapult Limited.

We must additionally find a way to reduce our reliance on contracting out tasks that do not allow the Department to develop internal expertise.

What I am concerned about is making sure that, first, the VA IT has an interoperable model in place; second, best practices should be in place from the private and public sector; and, third, that new IT strategies have the best value for our veterans.

Additionally, we must ensure we have a clear strategic plan that will be for the entire course. We have too often canceled a program or contract after many millions of hard-earned taxpayer dollars have been spent.

Finally, I encourage the VA to keep us updated on your efforts as we work jointly to give our veterans the 21st Century relevant IT system that they deserve.

Thank you, Mr. Chairman. I yield back.

[The prepared statement of Congressman Donnelly appears on p. 24.]

Mr. JOHNSON. I thank the gentleman for yielding back.

And I welcome the first panel to the witness table. On this panel today, we will hear testimony from the Honorable Roger W. Baker, Assistant Secretary for Information and Technology and Chief Information Officer (CIO) at the Department of Veterans Affairs.

Assistant Secretary Baker is accompanied by Peter L. Levin, Ph.D., Senior Advisor to the Secretary and Chief Technology Officer (CTO) at the Department of Veterans Affairs.

Assistant Secretary Baker, your complete written statement will be made a part of this hearing record and you are recognized now for 5 minutes.

STATEMENT OF HON. ROGER W. BAKER, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, AND CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY PETER L. LEVIN, PH.D., SENIOR ADVISOR TO THE SECRETARY, AND CHIEF TECHNOLOGY OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS

Mr. BAKER. Thank you, Mr. Chairman and Ranking Member Donnelly, for inviting me to testify in front of this Committee to discuss the Department of Veterans Affairs' information technology strategy for the 21st Century.

I appreciate the opportunity to testify on our plans, actions, and accomplishments on making VA's IT organization a 21st Century leader in the Federal Government.

As you said, Mr. Chairman, I am pleased to be accompanied today by Dr. Peter Levin, the CTO for the Department of Veterans Affairs.

I will be brief in my oral remarks. My written testimony provides details on the transformation we have been working to achieve in VA IT. And I believe the next panel will accurately depict a few of the many challenges that we faced when I was confirmed nearly 2 years ago.

Since that time, we have made substantial progress in the areas of customer service and customer satisfaction, product development, information security and privacy, financial tracking, and operational metrics.

Most importantly, we know that we have made progress due to the metrics that we now track and report in each of those areas. We have begun to operate VA's IT organization like a private-sector IT organization.

But we also clearly have a long way to go in achieving our goal of being the best IT organization in government and comparable with large scale private-sector IT shops.

While our metrics support our transformation, they also expose areas where much more work is required. So let me just touch on a few.

We must implement a technical reference manual or a TRM for our architecture and the processes to govern the specifics of what hardware and software is allowed to run in our expansive IT infrastructure.

Today we have over 64,000 different software packages that run on our desktop computers. Our visibility of the desktop initiative has allowed us to see exactly what runs on each of our desktop computers.

And I doubt that products such as Pinball Wizard have a medical use.

We must reduce the number of servers we support. From my private-sector experience, virtualization and elimination of physical server count can produce substantial operational savings.

And we must better define and rationalize our architecture at all levels, including our network, our data centers, our servers, our ap-

plications, our desktops, our help desk architecture, our product and use of support architecture, and at higher levels our medical business architecture, our benefits business architecture, and our corporate business architectures.

And we must ring efficiencies out of our application support area by pursuing shutdown of redundant or unused systems.

Finally, Mr. Chairman, we must find better ways to communicate with and motivate our IT employees because it is only through skilled and motivated employees that VA IT will achieve our goal as we seek to build an IT organization that can be compared with the best private-sector companies.

In closing, I would like to thank each of you again for your continued support of our Nation's veterans, of the Department of Veterans Affairs, and of VA IT. And thank you for the opportunity to testify before the Subcommittee on the important work we are undertaking to improve the results of VA's IT investments.

I look forward to your questions.

[The prepared statement of Mr. Baker appears on p. 24]

Mr. JOHNSON. Thank you, Assistant Secretary Baker.

We will now begin questioning and I will start off.

Does VA have an IT architecture that defines the blueprint for each of the 16 initiatives that is linked to business outcomes?

Mr. BAKER. Thank you, Mr. Chairman.

I do not believe I would tell you today we have a fully documented detailed architecture in that relative to any part of our organization. We have in the past had what I would call a shelf-ware architecture in the organization, meeting requirements, but not really guiding where we were going.

We have recently put one of our brightest folks in charge of the architecture area to renovate that, Dr. Paul Tibbits. I would say fortunately one of the first challenges Dr. Tibbits had was to be a key player in achieving the joint common electronic health record system with the Department of Defense.

Mr. JOHNSON. Let's go into that a little bit. Did I understand you to say correctly, and correct me if I am wrong, that you really do not have a complete architecture of VA's IT environment?

Mr. BAKER. That is absolutely correct.

Mr. JOHNSON. That is correct. Is it your opinion that an architecture that describes the VA business systems environment would be a first and critical component of developing an IT strategy?

Mr. BAKER. No. Actually, Congressman, I would not. And it goes back kind to the analogy of the alligators in the swamp. There are a lot of alligators in the VA IT infrastructure.

As you know, we were consolidated as an IT organization about 3 years ago. And a lot of the issues that we faced have been along the lines of just getting the basic changing analogies, blocking and tackling right inside the IT organization.

Mr. JOHNSON. I can relate to that. I have done that in the commercial world. But I also know that if you do not know where you are going, any road will get you there.

How many systems do you have in VA in IT? How many systems do you guys support?

Mr. BAKER. Speaking from an application system perspective, the best estimate I would give you is in the 400 to 500 range. I know

that we support approximately 300 of those in our Austin Information Technology Center or the Corporate Data Center Office. Most of our systems are going to be supported there and then other systems throughout the organization. So I think 500 is a reasonable estimate.

Mr. JOHNSON. Do you have a lead integrator that is linking the 16 initiatives and the associated projects to ensure consistency, standardization, and that these systems are going to talk to one another?

Mr. BAKER. We do not have a contractor from that perspective, no.

Mr. JOHNSON. Who is handling the integration effort?

Mr. BAKER. We have a member of our architecture team embedded with each of the major initiatives and we have the major initiative lead from an IT perspective working together to ensure that we are doing things that work together from the major initiative perspective.

Mr. JOHNSON. Do you have a timeline for developing an IT architecture?

Mr. BAKER. I could not give you one off the top of my head today, Congressman. I know Dr. Tibbits is working that right now. And to be clear, there are many facets of the IT architecture.

As I mentioned in my oral testimony, the first thing we are working on right now is the technical reference manual, something that then governs exactly what is allowed to run in our infrastructure as, if you will, a baseline from there. We are working on architectures in the areas of networks.

So, for example, we know where all of our circuits are. We know what our basic architecture at the network level is. But looking forward, we need a forward-looking network architecture and not a backward-looking circuitry of an architecture.

Mr. JOHNSON. You and I certainly agree on that regard. I am encouraged when you talk about virtualization because I have undertaken massive virtualization programs in the commercial world. And I can tell you that it brings tremendous benefits and cost savings.

How many data centers does the VA have?

Mr. BAKER. I believe that the report that we have given OMB says, I think it is 62 at this point.

Mr. JOHNSON. What is your life cycle replacement process for replacing the servers? How many servers do you have in those data centers?

Mr. BAKER. Right now the best number I have to give you and we are trying to define between virtualized instances and physical instances——

Mr. JOHNSON. Physical servers.

Mr. BAKER. My problem is today I know the number 37,000. Some of those are virtual on top, you know, multiple virtual on top of a single physical.

Mr. JOHNSON. Well, we are going to come back to this probably in a second round of questioning. I have some others. But I am going to defer to my colleague, Mr. Donnelly, now to ask his questions, but we will come back.

Mr. BAKER. Thank you, Mr. Chairman.

Mr. DONNELLY. Thank you, Mr. Chairman.

In looking at the Catapult contract, when you say that the acquisition team established a very aggressive timeline for the acquisition process and 236 sites, 45 are done, the cost overruns are staggering.

What was the decision framework used? I mean, how was that done that you wound up in a contract where it was not fully delineated, all the details were not there, all the information to get this done? How do you jump off when it appears that not every T was crossed?

Mr. BAKER. Thank you, Mr. Congressman.

That contract was awarded well before my time.

Mr. DONNELLY. Well, I understand.

Mr. BAKER. But as I looked at that contract, there are some mitigating parts of that. One of the things that is clear is that we, the government, underestimated the amount of concrete and metal in our hospitals.

Our goal in that WiFi contract was to prepare the way for advanced medical equipment that could be completely untethered from the wall and so we looked to provide 100 percent coverage and strong coverage for a WiFi signal inside of our hospitals.

It is fairly, I have to say, well-known physics that thick concrete and metal structures will block the signal and require more points of presence to accomplish that level of coverage.

My understanding is that that was the major cause of escalation in that contract was the underestimate of the number of points of presence that would be required in each facility.

From that perspective, that is a reasonable reason for the contractor to increase the costs. We are asking them to do more work. So we have done a better job of understanding from site surveys and other studies that that was factually true. I believe so. And that would lead to a more accurate contract award at the time of award to the vendor.

Mr. DONNELLY. The contract itself had an engineering change request that permitted pricing modification.

I mean, is there a point where you say this is what we are going to give you and those are the funds you get and we expect you to do the job for those funds?

Mr. BAKER. Yes. The problem there is that the contractor's appropriate response then is, yes, and I will deliver exactly what I contracted for for those dollars.

And so if you go into a facility and what we ask them to do will give us 70 percent wireless coverage, it really does not make sense to even wire the facility because then I could not use those WiFi devices.

If a nurse is going to do bar code medication administration with a WiFi device, but 30 percent——

Mr. DONNELLY. Well, let me ask you this. As we sit here today, we have 45 sites done, I think, out of 236?

Mr. BAKER. The number I had in my head was about a third of our major hospitals were done.

Mr. DONNELLY. Okay. Are we even capable of giving specs for a contract on this at this point? Do we know what a hundred percent

coverage would entail and could you get a fixed price for something like that right now?

Mr. BAKER. I believe so. We have stopped the previous contract per the report and other advice provided. And we are moving forward with the award of a new contract based on site surveys done independently of the new contractor. We are going to take the lessons learned from the previous contract and move forward with a new contract. Specifically to your question, we ought to be able to get a firm fixed price that we do not have to issue change orders against from the vendor to accomplish what we want to accomplish.

Mr. DONNELLY. What kind of time frame are you looking at?

Mr. BAKER. Congressman, I do not have that off the top of my head, but I believe we could give you the detailed acquisition schedule in a response after the hearing.

[The VA subsequently provided the following information:]

> Target award date for the new Wi-Fi installation contract is First Quarter FY 2012, and projected timeline to complete award to all remaining VAMC sites is 12–18 months from award.

Mr. DONNELLY. And one other question. Has the VA done an analysis yet on long-term savings by using open source for the joint electronic health record?

Mr. BAKER. Thank you, Congressman.

Yes, we have. And it goes down this path. We run one of the best electronic health record systems in the country right now, but we have proven that the normal methods available to the government to improve that system are not going to keep it up with the rate of improvement in the private sector.

We know from other folks' experience that in a number of years, and I peg it at 5 to 10 years, if we do not substantially improve VistA, my successor will be back here asking for somewhere around $16 billion to replace VistA in the hospitals. We must run a good electronic health record system in the hospitals. The benefits from a health care standpoint for veterans are outstanding and well proven.

Our move to open source is an attempt to use private-sector methods to bring the private sector much more into how we improve VistA and forestall or completely avoid having to pay a massive bill to replace VistA. If we can improve VistA and the costs for that incrementally are minimal, then we can avoid a huge out-year expense to replace it.

Mr. DONNELLY. Thank you very much.

Thank you, Mr. Chairman.

Mr. JOHNSON. Thank you, Mr. Donnelly.

Mr. Roe.

Mr. ROE. Thank you, Mr. Chairman. Just a couple of questions.

One, how big is this system when you look at DoD and how many people are we covering and just how enormous is this system?

Mr. BAKER. My understanding of the metrics is that between the two organizations, we have about 15 million annual patients covered by the two electronic health record systems. Probably between 15 and 20 million electronic health records inside the two systems.

I believe each system individually is among the largest health care organizations in the country. Both organizations were out in

front in adopting electronic health record systems. So singly we are huge. Jointly we are massive.

Mr. ROE. Well, the next question is, where are we timeline-wise? I have talked about this before, on getting this done because I think it is absolutely essential that you do not have two parallel massive systems that cannot talk to each other and it is obvious they are not going to be able to talk to each other? So where are we in that timeline?

Mr. BAKER. Congressman, Secretaries Shinseki and Gates absolutely agree with you. They have put us on a path to achieve a single common electronic health record system. I cannot get out in front of their communication relative to their May 2nd meeting. I can tell you, though, that our organizations have been working together for about 6 months.

The most important thing the two secretaries did was to agree that no is not an answer. The answer is yes and our organizations should figure out how to make that happen. That has come together very nicely.

I really have to not go any further than that in order to not get out in front of the secretaries, but we are very——

Mr. ROE. Let's get down a little bit more. When we had the changeover, when Secretary Panetta will be there, I do not know whether he has been brought up to speed or not. My concern is, he is going to be drinking from a fire hose when he first gets there. I mean, he really is.

And where is this priority? I do not want to sit here 2 years from now and we are having the same conversation because we get lost. I mean, he is going to be looking at three wars, I guess, now and all the other things that he is going to be doing in his new shop. And it is the infrastructure just below him to keep this ball rolling down the road.

Mr. BAKER. I believe I could safely say that that concern exactly 6 months ago from Secretary Shinseki's perspective is what kind of lit this discussion off.

I believe our objective and what we will accomplish is to have this nailed down before Secretary Gates leaves. We expect that Secretary Panetta will also be interested in it. But I know from the experiences Dr. Levin and I have had with working with the DoD that this has moved well beyond Secretary Gates into their organization at this point.

Mr. ROE. Good. I think that is essential because I think once you get the momentum, it will happen.

Do you have any time frame that you can think of that this could—I mean, is it a year, 2 years?

Mr. BAKER. Congressman, I just have to not get out in front of the secretaries on that one. I apologize. We are moving as quickly as we can and very hard. I expect a communiqué from them here in the next week or so that we will be able to give you more information.

Mr. ROE. Okay. And I guess the other thing I would like to know since we had the sort of loss of data, is this data stored in secure servers off site? How is the data backed up, because I know when we put our ERM in, that was a huge issue about where the data

is stored and if you have a crash, can you operate your system? In other words, if it is down, what do you do?

Mr. BAKER. Let me start with the metrics. We have a very good track record on availability of VistA systems. It is about 99.95 percent availability nationwide.

To the data question, the VistA systems today run in VA data centers. In half of the country, we have achieved consolidation of those systems into regional data centers. We will have 11 or 12 hospitals supported from a single data center. All the data is stored there and backed up there and retained there. The local facility has a read-only version of that data in case there is an outage to back up.

In the other half of our systems, the VistA systems hospitals, the VistA systems still run in the hospital and they back up locally there at their facilities.

Mr. ROE. Well, my time is up, but does DoD do the same thing?

Mr. BAKER. I am not familiar enough with DoD's setup to really answer that question right now.

Mr. ROE. Okay. I yield back.

Mr. JOHNSON. Thank you, Dr. Roe.

I want to go back to something that came out of Mr. Donnelly's questioning and correct me if I am wrong. He asked you if you have a cost analysis, cost-benefit analysis for your open-source decision.

And I understood you to say that you do; is that correct?

Mr. BAKER. At this point, we do, Congressman, yes.

Mr. JOHNSON. Well, I am curious because in previous conversations that we have had with you, Mr. Secretary, you said you did not have that.

Mr. BAKER. At that point in time, we did not. Based on——

Mr. JOHNSON. But, yet, you have already talked to the industry about your decision to move to open source.

Did you have that cost analysis before you made that decision? I mean, what good does a cost analysis, cost- benefit analysis do if you are going to make the decision before you get it?

Mr. BAKER. Well, as I discussed, I cannot remember if you and I had this discussion or if it has been with your staff, the cost-benefit analysis on open source is pretty straightforward.

Mr. JOHNSON. Can you provide that to us?

Mr. BAKER. Yes.

Mr. JOHNSON. All right. We can get it this week?

Mr. BAKER. Yes. We can provide it to you this afternoon.

Mr. JOHNSON. Okay. We would like to see that.

[The information provided to the Subcommittee staff was inadequate.]

Mr. JOHNSON. Let me go back to the data centers question again. You said you have 62 data centers, approximately 37,000 servers, correct?

Mr. BAKER. Yes.

Mr. JOHNSON. I hate to drill down into some technology stuff, but I have a method to my madness here. That equates to 596 physical servers per data center on the average. Does that sound right to you?

Mr. BAKER. I think to go back to the answer, the issue with the 37,000 number that I just discovered this morning as I was asking my staff is we think that some amount of that is actually counting virtual instances, multiple virtual instances that run on a single physical server.

Mr. JOHNSON. Yeah. So do you know how many physical servers you have in your network?

Mr. BAKER. Today I do not have that answer. Yesterday when I prepared my testimony, I thought I had that answer for you.

[The VA subsequently provided the following information:]

> As noted at the hearing, VA has around 37,000 virtual servers. The number of physical servers is 12,235.

Mr. JOHNSON. See, an architecture would tell you that. And the first step in managing an environment as complex as yours is, as costly as the VA's is, that would be a very, very first step because with virtualization, as you said, some organizations are seeing anywhere from 50 to 70 percent reductions in physical servers.

What is your life-cycle replacement strategy for servers?

Mr. BAKER. It depends on the server type. In general, we would like to replace them in the 4 to 6 year time frame. We have some, for example, the database servers on the VistA systems, that are well beyond that service period.

Mr. JOHNSON. How much on the average does a physical server cost, the type that you guys use? And you may use multiple types of servers, but as a general rule, do you have any idea?

Mr. BAKER. The best number I have for you there, sir, is about $10,000 each.

Mr. JOHNSON. Okay. All right. Let me go back. Do you have any metrics to measure your progress along these 16 initiatives? Do you have any metrics that will tell you whether or not you are achieving the goals? I mean——

Mr. BAKER. Yes.

Mr. JOHNSON. You do?

Mr. BAKER. Each and every one of the 16 major initiatives has an operating plan agreed to with the Deputy Secretary. The Deputy Secretary manages each of those initiatives on a monthly basis to their operating plan. So we look at are they achieving the milestones and results at the initiative level.

Underpinning that then are specific IT projects that are managed to the milestones for those IT projects and whether they are making those inside of the Program Management Accountability System (PMAS).

Mr. JOHNSON. How many different functional areas does your IT department support within VA? I mean, you have financial applications, I am sure. You have various health applications. What different functional areas?

In a manufacturing company, you would have operations, you would have finance, you would have purchasing, you would have all of those different things. What are the different functional areas that your department supports?

Mr. BAKER. So from an IT perspective, we look at our customers inside the organization in three areas. There is the health portfolio, there is the benefits portfolio, and there is the corporate portfolio systems.

So in corporate would be human resources and finance, the contract management system, those sort of things.

In the benefits portfolio would be each of the systems necessary to support the various pieces of the business of the Veterans Benefits Administration, so education, compensation and pension, loan guarantee, and also national cemeteries with their electronification.

And then in the health portfolio, the main items are the automation systems in the hospitals, but there is also a financial portfolio inside of health for their business office. I think that is probably a fairly reasonable view of the overall portfolio.

Mr. JOHNSON. And theoretically all of those systems pass information back and forth one to another, right?

Mr. BAKER. We sure wish they did a lot more of it, sir, yes.

Mr. JOHNSON. Back to my concern about architecture. Is open source on the multi-year program?

Mr. BAKER. Yes.

Mr. JOHNSON. Okay.

Mr. BAKER. As I understand the question.

Mr. JOHNSON. Okay. Well, you know, I am going to sort of summarize with this.

Mr. Donnelly, do you have any other questions?

Mr. DONNELLY. No more questions.

Mr. JOHNSON. You know, I have heard your testimony this morning, no architecture, no timeline for an architecture. When asked by Dr. Roe if you have a timeline for EHR integration with DoD, there is no timeline for that.

I am just really confused and concerned about how the taxpayers' resources are being used and the level of support that we are providing to our veterans.

You have some 7,000 people in the IT department within the Veterans Administration. I am trying to equate that to my experience.

I know in 1992, the United States Air Force's Software Development Center had roughly 2,000 people to develop all of the software, maintain that software for the entire portfolio for the air force, everything from food service to dropping bombs.

I just find it hard to believe that with an architecture and an understanding of how these systems should be integrated together that we could not find cost savings, resource efficiencies. And I know you are nodding in agreement and some of your testimony indicates that you want to get there.

Why is it taking so long? How long have you been there?

Mr. BAKER. Next week will be 2 years.

Mr. JOHNSON. Why is it taking so long because you are not the first that this committee has had these types of discussions with? This seems to be an ongoing thing.

I told someone the other day I feel a little bit like a greyhound at a dog track. We come out and then we chase these rabbits around from one session of Congress to the next. We put the rabbit up and then the next session, we bring the rabbit out. We chase him around again and we get many of the same answers over and over and over again.

I think the American people, I think America's veterans deserve better than that.

Why is it taking so long to get our arms around architecture, around common-sense business practices, around project management, concepts like virtualization that has been around for years now? Why is it taking so long, Mr. Secretary?

Mr. BAKER. Congressman, in a much longer discussion, I would love to have that discussion, but——

Mr. JOHNSON. We have plenty of time. I mean, we have the hearing room until noon to hear what your comments are.

Mr. BAKER. Let me answer it this way. I do not believe that I have established a reputation for sitting around. We introduced PMAS, the Program Management Accountability System, within 1 month of me——

Mr. JOHNSON. Mr. Secretary, I asked you very specific questions around architecture, around common-sense project management, business practices, things like cost-benefit analyses coming out after the fact.

Why is it taking so long to get common-sense IT strategic planning processes in place within the Veterans Administration?

Mr. BAKER. The simple answer, Congressman, is that the government clearly does not operate like a private-sector organization. None of the disciplines that I think are necessary for an IT organization existed inside of VA IT. The way it had been run before I arrived was not in a way a private-sector organization would be organized or run.

We have implemented strong financial disciplines. I pulled $700 million out of VA IT and saved that money to spend it in better places because, frankly, when I arrived, that money was being wasted.

We have a good track record of focusing on it. I understand your focus on architecture. I would like to get there. But the problems we faced when we came in that you are about to hear about from the next panel, failing $127 million programs like replacement scheduling, had to be dealt with, had to be dealt with soon so we did not continue to waste the taxpayers' dollars.

Mr. JOHNSON. Well, you have got——

Mr. BAKER. I agree with you on architecture, sir. I do not disagree with you. I think our only difference is in the perspective on what things are going to bite us hard first.

As we both know, a VistA system down in a hospital is critical and I had to make certain that that would not occur. I had to make certain that information loss was stemmed, that we would not have issues in those areas.

I had to stop our failing IT programs that were wasting hundreds of millions of dollars of taxpayers' money.

I agree with you on architecture. I would love to get there. I believe it is a matter of prioritization and just the way that I look at an IT organization.

Mr. JOHNSON. I commend the fact that you recognize that some of these problems exist. I mean, that part is encouraging.

I will leave you with this. I remain concerned that we do not have an overall 30,000-foot view of the VA's IT environment, how these systems interconnect, which system is required to talk to another system, and how we are utilizing the millions of dollars that

are being spent on IT within VA, and what we are doing with those 7,000 people.

I think the American taxpayer is asking for answers around that. You well know, you hear it every day America is broke. We have to find a way to do things better, to do things more cost effectively.

And, you know, from my perspective, and I hear you say that you recognize some of those, IT is one of the most costly aspects of any organization's cost basis today, in today's environment. There is no question about that. It is also the place where the most savings can be recognized with sound, common-sense best practices, those kinds of things.

And so I thank you for your testimony today. I am going to encourage you to stay around——

Mr. BAKER. We will be here.

Mr. JOHNSON [continuing]. And listen to the next panel. And with that, you are excused. Thank you very much.

Mr. BAKER. Thank you.

Mr. JOHNSON. Well, I invite the second panel to the witness table. On this panel today, we will be hearing testimony from Belinda J. Finn, Assistant Inspector General for Audits and Evaluations at the VA Office of Inspector General (OIG).

Ms. Finn is accompanied by Ms. Maureen T. Regan, Counselor to the Inspector General at the VA Office of Inspector General.

We will also receive testimony in this panel from Joel Willemssen.

Am I pronouncing that right?

Mr. WILLEMSSEN. Yes, sir.

Mr. JOHNSON. Okay. Managing Director for Information Technology at the U.S. Government Accountability Office.

Ladies and gentleman, your complete written testimony will be made part of the hearing record. We will begin with Ms. Finn.

You are now recognized for 5 minutes.

STATEMENT OF BELINDA J. FINN, ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY MAUREEN T. REGAN, COUNSELOR TO THE INSPECTOR GENERAL, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND JOEL C. WILLEMSSEN, MANAGING DIRECTOR, INFORMATION TECHNOLOGY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF BELINDA J. FINN

Ms. FINN. Thank you, sir.

Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the OIG's findings regarding VA's management of its information technology projects.

Ms. Maureen Regan, Counselor to the OIG, is also here today.

Our testimony summarizes our recent work highlighting issues regarding VA's IT governance and system developments.

During our audit of VA's IT capital investment management, we examined VA's realignment of its IT program from a decentralized to a centralized management structure.

We reported that the ad hoc manner in which the Office of Information and Technology or OI&T managed the realignment had resulted in an environment with inconsistent management controls and inadequate oversight.

Further, in September 2009, we reported that VA needed to manage its major IT development projects in a more disciplined and consistent manner.

In general, VA's processes were adequate. However, OI&T had not communicated them, complied with them, or enforced the software development requirements.

Our audit work on several IT development projects has identified problems with inadequate project and contract management, staffing shortages, and lack of guidance. These recurring themes have repeatedly hindered VA's IT development success.

Our reports on the Financial and Logistics Integrated Technology Enterprise Program, better known as FLITE, concluded that program managers were repeating problems from the failed CoreFLS Project. Specifically the FLITE Program managers did not have requirements, plans, and controls to ensure the achievement of cost, schedule, and performance goals, have sufficient staff or clear roles and responsibilities, and effectively identify and manage the risk associated with the Strategic Asset Management Pilot Project.

OI&T has since suspended the Pilot Project for not meeting user acceptance requirements.

Our report on the Post-9/11 GI Bill long-term solution concluded that OI&T met schedule deadlines while sacrificing cost and performance objectives. Lacking the management, discipline, and processes for effective project development, future long-term solution releases to meet mandates of the revised GI Bill could meet the schedule, but at the expense of cost and performance goals.

Our report on the Veterans Services Network Project, VETSNET, concluded that, given the competing priorities, VA's plans and schedule for migrating all programs to the new system, the VETSNET System, were unclear.

Work to meet the original program objectives had been extended by 5 years and at a cost of $308 million are more than two times the projection from 2006.

OI&T has historically struggled to manage IT acquisition contracts effectively. In response to a hotline complaint, we reviewed a contract to install wireless networking services at 236 VA sites. We found the time frames to plan, solicit, and award the contract were unreasonable.

VA had also issued a statement of objectives without enough detail for vendors to submit reasonable proposals resulting in escalating contracting costs and delayed network installation nationwide.

In conclusion, the Department historically has struggled to meet IT development cost, schedule, and performance objectives. We are currently reviewing OI&T's new Program Management Accountability System to assess the controls that are needed to improve program oversight and ensure success in development efforts.

Mr. Chairman, thank you again for the opportunity to be here today. Ms. Regan and I would be pleased to answer any questions that you or other Members may have.

[The prepared statement of Ms. Finn appears on p. 31.]

Mr. JOHNSON. Thank you, Ms. Finn.

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

STATEMENT OF JOEL C. WILLEMSSEN

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Ranking Member Donnelly. Thank you for inviting us to testify today on VA's management of information technology.

As requested, I will briefly summarize our statement.

Our work at VA over the last several years has shown that the Department faces challenges in effectively managing IT. Today I will cover three of those.

One, developing information systems; two, securing information and systems; and, finally, working with the Department of Defense to implement joint solutions.

Regarding developing systems, we have recently reported on two important VA systems development projects. VA began work more than a decade ago on the first project, an effort to replace the Outpatient Appointment Scheduling System that the Department said had long-standing limitations.

However, after spending an estimated $127 million over 9 years, VA had not implemented any of the project's planned capabilities. The effort was hindered by weaknesses in several key management disciplines such as acquisition planning, requirements analysis, testing, progress reporting, risk management, and oversight.

We made recommendations to VA in each of these areas to improve future development of needed capabilities.

We also reviewed VA's development of a new system for processing Post-9/11 GI Bill educational assistance benefits. In this case, we found that VA had delivered initial key automated capabilities and was, therefore, able to provide regional processing offices with the capability to prepare benefits claims.

However, we also identified areas for improvement and made several recommendations to VA to further guide full development and implementation of the entire system.

Let me next turn to a second major VA challenge, information security. Long-standing weaknesses in security controls have consistently been a material weakness at VA. We and the VA OIG have issued numerous reports showing that these weaknesses are pervasive and place VA's program and financial data at risk.

Implementation of the many recommendations directed to VA and a fully effective information security program are critical to the Department reducing its security risks.

Finally, let me highlight the barriers that VA faces in establishing shared electronic record capabilities with the Department of Defense.

VA and DoD each have massive health care operations and each spend large sums of money to separately develop and operate electronic health record systems.

Earlier this year, we reported that due to barriers in three key areas, VA and DoD lacked mechanisms for identifying and implementing IT solutions to jointly address their common health care system needs.

These barriers were, one, strategic planning that jointly addressed requirements; two, enterprise architectures to guide how they would move to an integrated set of systems; and, three, investment management processes that would help ensure that chosen solutions would meet the departments' common needs and provide better value to the government as a whole.

We recommended several actions to the secretaries of Veterans Affairs and Defense to overcome these barriers. Both departments concurred with our recommendations and in March of this year, the secretaries committed their respective departments to pursue joint development of integrated capabilities. Doing so can lead to better solutions at lower cost.

That concludes a summary of my statement and I look forward to your questions. Thank you.

[The prepared statement of Mr. Willemssen appears on p. 36.]

Mr. JOHNSON. Thank you very much.

Ms. Finn, you mentioned in your testimony that they have adequate oversight processes, right? Did I understand that right?

Ms. FINN. I believe what I referred to was that the policies and procedures for system developments seemed adequate in that they reflected the commonly accepted best business practices for system developments.

Mr. JOHNSON. Okay. But, yet, you indicated that the problem was with compliance with those processes?

Ms. FINN. Yes. The issue was compliance with those processes and the implementation of them. To be specific, the way they had been promulgated throughout the Department sometimes gave managers the impression that they were just guidance and, therefore, not something that they needed to follow or should follow, but were suggestions.

Mr. JOHNSON. Did you see any evidence of any emphasis on the compliance issue? I mean, did they have processes in place to identify lack of compliance and mitigating action once they discovered it?

Ms. FINN. Our audit work was about 2 years ago and at that time, no, the process did not have a lot of structure and discipline to it.

Mr. JOHNSON. Okay. Mr. Willemssen, you mentioned three areas, development of IT systems, security, and joint integration.

Is it your opinion, and I thought you said so, I just want to clarify, that an architecture that clearly indicated how all of these different systems would fit together and a road map for integrating them would be a major step in the right direction to overcome those inadequacies?

Mr. WILLEMSSEN. Absolutely, Mr. Chairman, absolutely critical to doing so. And I understand the magnitude of what the Chief Information Officer is facing. And given that magnitude, he probably has to take it in doable bites and look at the most critical functions and make sure he understands the architecture of that. And most importantly, where does he want to go.

Mr. JOHNSON. Okay.

Mr. WILLEMSSEN. And that is why we focused, for example, on the VA and DoD area, that jointly, they need to figure out where they want to go, figure out where they are, and then have a transi-

tion plan to get from here to there. That is what is currently missing.

We are encouraged, though, by the recent announcement that the secretaries are committed to this, but you are right. Constant oversight by your Committee among others will go a long way to making sure that happens. Without that oversight, things can fall by the wayside.

Mr. JOHNSON. Well, Ms. Finn mentioned compliance with processes and you talked about the lack of an architecture.

Is it your sense that, Mr. Willemssen, inside the VA, do they really have an understanding of the software development life cycle and the major steps involved because you mentioned development specifically? Did you find in your analysis that there is understanding of the software development life cycle?

Mr. WILLEMSSEN. It is a mix. With the size of the organization, there are elements that do understand the life cycle. There are elements who clearly, for example, understand the Software Engineering Institute's capability maturity model and are striving to do as best as possible within the parameters of the engineering disciplines within the model. But that is not prevalent throughout the organization——

Mr. JOHNSON. Okay.

Mr. WILLEMSSEN [continuing]. So that when you are going with any particular system development effort, it is somewhat hit or miss and, therefore, the software development processes may not be ingrained, but it may be ad hoc and chaotic. You may get lucky and you may have a group that knows what they are doing. On the other hand, you may not.

Mr. JOHNSON. Did you see any indication or evidence that there is a formal program management or project management certification program within the VA with how their IT projects are run?

Mr. WILLEMSSEN. I do not recall that, but that is something that Mr. Baker, I believe, is pushing very hard and that we would be supportive of. But we have not done work specifically on project management, but I think you are definitely on the right topic there because it continually comes up in the systems that we have reviewed.

Mr. JOHNSON. It goes back to what I said earlier. I mean, if you do not know where you are going, any road will get you there and so we end up with what we have.

We will probably come around for another second round of questions to you folks. I appreciate it.

I will yield at this time to Mr. Donnelly.

Mr. DONNELLY. Thank you, Mr. Chairman.

Mr. Willemssen, have you sat with the DoD and talked to them about this issue and asked what their positions are and what they plan to do?

Mr. WILLEMSSEN. We have. We have also done an in-depth review of their AHLTA (Armed Forces Health Longitudinal Technology Application) System which is their own health care system. Again, I am encouraged by both secretaries committed to do something because without that, you are going to want to continue to go with your own Department's system.

Mr. DONNELLY. What do you plan your continuing role to be in making sure this progress continues to see that it is not two home teams doing their own thing?

Mr. WILLEMSSEN. At this point, our plan would be to follow-up on our outstanding recommendations that we made in our February report in those three barrier areas that I mentioned.

And also before the hearing, Dr. Levin and I committed to meeting within the next 2 weeks to get further understanding of what is going on subsequent to the secretaries' commitment to pursue this aggressively.

Mr. DONNELLY. Do you have your own progress schedule for a timeline on this integration and this coming together so we can have a system that works across both departments and that work seamlessly with one another?

Mr. WILLEMSSEN. We do not have a specific schedule other than following up on the recommendations and providing periodic progress reports to bodies such as this that provide oversight. So if I were to come here a year from now and report the same information, that would definitely say something.

Mr. DONNELLY. Do you have any idea cost-wise if both groups were on the same plan, following the same software and working together so the records come over seamlessly from DoD to VA that were able to track individuals, what kind of cost savings that would result in?

Mr. WILLEMSSEN. We have not done the cost analysis. But when you look at the billions that are planned to be spent on each separately over the next many years, I think you can see the opportunities for savings are significant. You overlay on that plans that not only VA has but DoD and the rest of the Federal Government to significantly consolidate the massive number of data centers that are out there and you will have again tremendous cost savings.

Mr. DONNELLY. Ms. Finn, you have identified a number of programs that there is a lack of sufficient or qualified IT personnel.

What can be done to address this problem in your judgment?

Ms. FINN. This is the case I think where OI&T will have to have a concerted strategy and an implementation plan to address that issue.

When Mr. Baker first started and he and I first met, he asked what do you think my biggest problem will be. And I said system development without a question and he agreed. And he has worked to address that.

I will be able to tell you a little more specifically about what the Department needs to do later this year. We are planning to do an audit of OI&T's human capital management and we will probably be looking at their strategy and implementation for increasing their expertise in program management.

Mr. DONNELLY. And one final question is, from your perspective, what exactly has the VA done now to improve its ability to manage IT projects and what do you think is the most important thing they can do to improve that?

Ms. FINN. They have taken two actions. One is the use of the Agile system development methodology which calls for incremental functionality little bits at a time and that allows a project to hopefully make better progress than the traditional waterfall method

that, you know, assumes you have everything planned out before you start.

And the second is the Program Management Accountability System, which is the oversight structure that OI&T uses to monitor the progress of all their system development efforts in the various projects.

PMAS was somewhat of a departure for VA in that it provides an overarching look at system development. We have been doing some work to actually look at the implementation of the PMAS system and the discipline because, as you know, often the devil is in the details as to how well the oversight is implemented. And we will be issuing a report on that later this summer.

Mr. DONNELLY. Thank you very much.

I yield back, Mr. Chairman.

Mr. JOHNSON. Thank you.

Ms. Finn, you mentioned the Agile implementation methodology. And I have used that myself and so I agree with you that it is a good way especially on big projects.

However, you know, I am going to keep beating this horse until we get someone's attention. Architecture, Agile works well when you have a well-defined set of requirements, a well-defined road map on where you are going to.

Is it your opinion that Agile works well in environments where you really do not have that, where you do not know which way you are going?

Ms. FINN. I do not think any software methodology can work if you do not really have an end game in mind to know what you are trying to develop. And I would think Agile has no more advantage in that situation than the waterfall method.

Mr. JOHNSON. Sure. Okay.

Mr. Willemssen, the Ranking Member just started talking about some staffing deficiencies.

Do you feel that the VA OI&T staffing of over 7,100 people is appropriate and effective?

Mr. WILLEMSSEN. Appropriate? We have not done a detailed analysis of all the staff, what their capabilities are, how they are deployed, what they are working on, so I would not venture a guess on that.

I would say that based on my almost 20 years off and on of evaluating VA IT there are pockets of excellence and there are pockets where much additional work is needed. So it is hard to generalize.

I think what the Inspector General's representative said here about taking a look at the human capital function within IT and seeing what kind of capabilities, what kind of certifications, what kind of project management discipline, that makes a lot of sense.

And I think Mr. Baker would probably welcome such a review.

Mr. JOHNSON. Okay. Shifting back just a little bit and either of you can respond to this question, what would prevent VA OI&T from fully implementing the information security program required under the Federal Information Security Management Act of 2002 (FISMA)?

Ms. FINN. Big question there. No single thing comes to mind. Of course, we do review the information security posture annually

under the requirements of FISMA. In fact, our report on 2010 should be available fairly soon.

The biggest obstacle that I see is, and Mr. Baker may have a different thought on this, is VA's decentralized nature in that even with a centralized OI&T, a centralized information technology organization, you still need to have consistent implementation and disciplines out at many facilities.

Your security is only as good as, you know, as each individual location. And it is a very cumbersome process to identify all of the issues and have the command and control structure needed from Washington to make sure all of the fixes are made and updated because information security is a daily requirement. You have to keep your patches. You have to keep your passwords.

So it is the decentralized nature I believe is the big challenge and just the fact that you have to keep up with it every day in that environment.

Mr. JOHNSON. Okay. Do you think developing technologies such as cloud computing and open source, even though the U.S. Chief Information Officer has cited security concerns, do you have concerns about pursuing that given the security issues that we have already talked about?

Ms. FINN. Of course I have concerns. I was reading the Office of Management and Budget's strategies yesterday about cloud computing and I noted that they talked about establishing Federal clouds hopefully to provide better security That gives me a little more comfort than just going out to the commercial area. But I think even that environment will require a lot of monitoring and controls to ensure that it is secure.

At VA, of course, we deal with a lot of personal information and so we want to make absolutely certain that it is secure.

Mr. WILLEMSSEN. If I may, Mr. Chairman——

Mr. JOHNSON. Absolutely.

Mr. WILLEMSSEN [continuing]. I would echo that issue. We issued a report last year on the Federal Government's plans to move forward with cloud computing. We were especially concerned at that time at the lack of guidance addressing the security ramifications of going to the cloud.

Since that time, there has been some guidance disseminated, but for an organization that has much sensitive data, you have to make that move very carefully and with a lot of controls in place with the provider of the service.

Mr. JOHNSON. Mr. Willemssen, we talked a little bit about, and I agree with you, it is encouraging to see that the secretaries of the departments have committed to moving forward with this joint development integration.

Can you explain to us why you think it took VA and DoD until March of this year to finally come to that commitment to joint development of that electronic health system?

Mr. WILLEMSSEN. Growing pressure to do so. I think the frustration was getting too high. And I think that frustration was starting to boil over and I think both departments began to recognize that they had to do something, especially given again what you said earlier.

We are a country that does not have a lot of excess funds to spend and you see the amount of money going into the health systems for DoD and VA and it looks like an easy opportunity to save some money and, oh, by the way, have better service to our servicemen and women and veterans. So this looks like an easy thing to do.

It is the institutional and cultural resistance historically to doing it. That is why I think unless you have somebody at the secretary level driving this, it is going to be very difficult to accomplish because of those institutional and cultural barriers.

Mr. JOHNSON. Yeah. Well, tough question here. What is your confidence level that, I mean, if they did not do this on their own out of their own capacity to see the need for it and they had to wait until there was so much pressure to do so, what is your confidence level that the departments are going to work well together and specifically how do you view the influence of each department over the Integrated Program Office in terms of moving the ball up the field and making progress because I still remain concerned about no timelines?

I have yet to see, maybe it exists, but I have yet to see a project management or a program management plan that says who is committed to do what tactically.

Mr. WILLEMSSEN. Absolutely. I agree with you. That is what we are looking for too. And I think if the secretaries' communiqué, as was mentioned earlier, is going to come out a week from now, those are the kind of details that we want to see and then hold the departments accountable to the details in that communiqué.

Mr. JOHNSON. Yeah. We will be watching for that very closely as well. It should reveal some specificity around how we are going to pursue this. It is the right thing to do for America's veterans. It is the right thing to do for the taxpayers.

With that, do either of you have any closing comments before we wrap up?

Mr. WILLEMSSEN. No, sir. Thanks, Mr. Chairman.

Mr. JOHNSON. All right. Well, my thanks to you then for joining us today. I appreciate your testimony.

Ms. Regan, you did not get a chance to say anything. Anything on your mind?

Ms. REGAN. No. I am fine. Thank you.

Mr. JOHNSON. Okay. Well, you are now excused.

I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and include extraneous material. And seeing as I am not going to object to my own motion, that is so ordered.

I want to thank all Members and witnesses for their participation in today's hearing and business meeting.

This hearing is now adjourned. Thank you all.

[Whereupon, at 11:14 a.m., the Subcommittee was adjourned.]

A P P E N D I X

Prepared Statement of Hon. Bill Johnson, Chairman, Subcommittee on Oversight and Investigations

Good morning. This hearing will come to order.

I want to welcome everyone to today's hearing "Reboot: Examining VA's IT Strategy for the 21st Century."

With an information technology budget exceeding three billion dollars annually, it is reasonable for the American taxpayer to expect the Office of Information and Technology at VA to effectively utilize available technology and provide the highest quality support in the Department's delivery of health care and benefits to veterans.

As we will hear from the witnesses on both panels today, billions of dollars have been spent on IT at VA. However, veterans, the taxpayers, and Members of this Committee are left to wonder what has resulted from these expenditures. Have improvements been made? Certainly. Are the improvements and advancements in VA IT over the last 10 years on par with the amount of time and taxpayer dollars put into the effort? Certainly not.

The witnesses on today's second panel will help illuminate the magnitude of the money spent on IT over time. To name a few: $127 million over 9 years on an outpatient scheduling system, with none of the planned improvements in place; suspension of the Strategic Asset Management, or "SAM" program, after failing to meet yet another milestone; and a $70 million overrun on a Wi-Fi installation contract.

I also remain concerned that, as with past contracts and efforts, VA is not thoroughly vetting cost and risk analysis before undertaking new, large IT projects.

While VA continues to push forward on cloud computing, its own Administration has not fully established the Federal guidelines for information security in cloud computing. In a health care environment such as VA's, I know that I would not want my personally identifiable information floating around in the "cloud", especially given a track record of data breaches that is less than stellar.

We once again notice a history of poor acquisition and contract management at VA, a theme this Subcommittee is familiar with. Given the frequency of problems in IT contracts, we know there must be a significant degree of inexperience among the contracting staff, but we are also left to wonder whether supervisors in OI&T either don't know or don't care about these shortcomings. When IT needs are not clearly defined at the beginning of the process, it leads to cost increases and time delays down the road.

With an IT staff of over seven thousand, I find it difficult to believe that knowledgeable IT professionals are not helping to create well-defined Requests for Proposal, a key element of a viable contract. When these contracts constantly have to be modified, it results in greater cost to the taxpayers and a delay of improved services to veterans.

A crucial area for VA IT to meet expectations is the establishment of the joint Electronic Health Record, or "EHR", with DoD. Yet another overdue item for our active duty servicemembers and our veterans, the EHR has been pursued separately by the two departments. The result is billions of dollars spent, much of it duplicative, and no joint EHR. While I commend the Secretaries of both departments for finally committing this spring to cooperatively pursue this endeavor, I have lingering concerns that mistakes made in previous IT contracts could be repeated.

For example, after releasing a final RFP on an Open Source custodial agent at the end of last month, VA is only allowing a 3-week turnaround for proposals to be submitted at the end of this week.

It's not rocket science. The capabilities to do what needs to be done already exist. Hundreds of millions of dollars could have been saved in previous years by simply having a robust IT architecture and strategy in place. The needs are clearly defined: protect veterans' information, establish an electronic health record *in conjunction* with DoD, and implement stringent oversight of these and all undertakings in the Office of Information and Technology. I fully understand the challenges of managing

information technology in a large organization. What I do not understand is why it has taken so long to get only so far at VA. The American people are watching, and expect VA to take care of our veterans as promised.

I appreciate everyone's attendance at this hearing and I now yield the Ranking Member for an opening statement.

Prepared Statement of Hon. Joe Donnelly, Ranking Democratic Member, Subcommittee on Oversight and Investigations

We often criticize the VA for their inefficient and outdated IT systems. A perfect example of this was when the VA found themselves having to process education claim manually due to the legacy system being unable to process education claims after the passage of a modern education program. For this reason, I find it important and critical that the VA maintains and updated IT system that proves to be reliable and can be manipulated as new software is incorporated through the years ahead.

The VA has decided that using Open Source model will provide a better outcome, with lower risks and lower cost. Their cooperation with the DoD on using Open Source is encouraging, in part because this cooperation is essential, there is a critical need to develop and electronic health record system, and because DoD has relied on Open Source in the past. Although there are multiple concerns that both the majority and the minority might share, the VA has reassured us that Open Source provides several benefits. But along with those benefits, making sure that veteran's personal information remains secure is critical.

I also understand that contract management and weaknesses have overshadowed VA's efforts to keep up with the VA's IT infrastructure. Cost overruns, contract weaknesses, and unmet project time frames are just a few examples of the implications that can occur if there are no firm requirements in contracts, such was the case with the Wi-Fi awarded contract to Catapult, Ltd.

What I am concerned about is making sure that first, the VA IT has an interoperable model in place; second, best practices should be in place from the private and public sector; and third, that new IT strategies have the best value for our veterans.

Finally, I encourage the VA to keep staff updated on your efforts.

Prepared Statement of Hon. Roger W. Baker, Assistant Secretary for Information and Technology and Chief Executive Officer, Office of Information and Technology, U.S. Department of Veterans Affairs

Introduction

Chairman Johnson, Ranking Member Donnelly, Members of the Subcommittee: thank you for inviting me to testify regarding the Department of Veterans Affairs' (VA) Information Technology (IT) strategy for the 21st Century. I appreciate the opportunity to discuss VA's plans, actions, and accomplishments that will position VA's IT organization as a 21st Century leader in the Federal Government.

I am pleased to be accompanied today by Peter Levin, Ph.D., VA's Chief Technology Officer.

Through Secretary Shinseki's leadership, the VA continues to focus on the strategic goals VA established 2 years ago to transform VA into an innovative, 21st Century organization that is people-centric, results-driven, and forward-looking. These strategic goals seek to reverse ineffective decision-making, systematic inefficiency, and poor business practices in order to improve quality and accessibility to VA health care, benefits, and services; increase veteran satisfaction; raise readiness to serve and protect in a time of crisis; and improve VA internal management systems to successfully perform our mission. The Office of Information and Technology (OI&T), which I am honored to lead, proudly support our strategic goals as we rapidly deliver technology to transform VA.

The VA IT enterprise is a massive single, consolidated network with 152 hospitals, 791 community-based outpatient clinics (CBOC), 57 benefits processing offices, and 131 cemeteries and 33 soldier's lots and monument sites. Our OI&T workforce numbers over 7,100, serving over 300,000 VA employees and more than 10 million veterans. Within our $3.1 billion FY 2011 budget, OI&T manages a technology profile of over 314,000 desktop computers, 30,000 laptops, 18,000 blackberries and mobile devices, and 448,000 email accounts. These figures describe an

IT enterprise that is certainly one of the largest consolidated IT organizations in the world.

Disciplines for 21st Century Information Technology

Managing an organization of this size and scope requires disciplined management and processes. To instill those disciplines, VA implemented five major focus areas immediately after my confirmation. These five areas—customer service, product delivery, information security, operational metrics, and financial reporting—continue to guide our efforts in a disciplined and measurable way.

1. Customer Service

OI&T continues to build upon our excellent relationships with VA's Administrations (Veterans Health, Veterans Benefits, and National Cemeteries). We have worked hard to set a tone of cooperation that has made it possible for us to effectively address many complex problems at the second largest agency in the Federal Government. Thanks to my partners, Dr. Robert Petzel, Under Secretary for Health, Mr. Michael Walcoff, Acting Under Secretary for Benefits, and Mr. Steve Muro, Acting Under Secretary for Memorial Affairs, that same cooperative approach continues to spread throughout VA.

2. Product Delivery

IT is an enabler to the implementation of the Secretary's 16 Transformational Initiatives, which cannot be executed without newly developed IT products. These initiatives are key to improving VA's services to Veterans, and IT investments have allowed us to deliver products or plan for on-time delivery of the following programs:

- *Successful, on-time delivery of the critical GI Bill project.* VA successfully converted all processing of new Post-9/11 GI Bill claims to the Long Term Solution (LTS) prior to the commencement of the Fall 2010 enrollment process. Since installation, processing with the new system has been excellent, with no significant "bugs" encountered. The Veterans Benefits Administration claims processors like the new system and find it easier and more efficient to use. By dramatically changing its development processes, adopting the Agile methodology for this project, VA also dramatically changed its system development results;
- *Veterans Benefits Management System* (VBMS), in which IT provides Veterans Benefits Administration the enabling technology to break the claims backlog;
- *The Blue Button program,* in which IT provides the systems and information security to allow Veterans to download their currently available personal health information from their MyHealtheVet account, allowing them to share their personal health information with doctors outside the VA;
- *The eBenefits portal* (a joint DoD and VA service), which is evolving to a "one-stop shop" for benefit applications, benefits information and access to personal information such as official military personnel documents;
- *Veterans Relationship Management* (VRM), in which IT will provide the capability to improve Veterans access to VA services and benefits through phone, web and email systems enabling easier and more effective communications; and
- *The Pharmacy Reengineering program* that replaces existing pharmacy software modules with new technology that will enhance Pharmacy services, improve customer service and enhance patient safety.

As these examples illustrate, IT plays a pivotal role in the transformation of VA into a 21st Century organization as envisioned by the President and Secretary Shinseki.

3. Information Security

Ensuring the security of the large VA network and devices is vital. We have made substantial progress in information security since the challenges experienced in 2006 by instituting controls that now provide for remote access to VA resources for employees and selected business partners, and implementing a sound security strategy to facilitate secure data exchange with Department of Defense and private-sector health care organizations, and facilitating access to electronic health records for our veterans over the Internet. These efforts are instrumental in making the administration's vision towards a virtual lifetime health record possible.

We have already made great strides with some efforts that will be discussed in greater detail below, including: visibility to the desktop to ensure compliance with security policies; visibility to every network device; strong user authentication; and medical device isolation architecture. It is vital to us that veterans feel confident that we are doing everything we can to secure their private information.

4. Operational Metrics

Our operations organization provides excellent service to our hospitals, benefits offices, and cemeteries. We now measure and publish key metrics that tell us how we are doing. Beginning in June of 2009, we started at the core, measuring network availability (which averages 99.99 percent), Veterans Health Information Systems and Technology Architecture (VistA) system availability (99.95 percent), and help desk wait times. We have expanded these measurements to include a list of nearly 167 metrics covering aspects of our network, our service provision and our system/application provisioning that help us understand what works well and what does not. The ability to measure these key processes and adjust accordingly is central to continuous operational improvement—a hallmark of a mature operation and essential to any 21st Century IT organization.

As an example, we recently completed our second enterprise-wide customer satisfaction survey, using the American Customer Satisfaction Index methodology, which allows us to compare our results to those of like organizations throughout government and industry. Our primary purpose in conducting this survey is to understand and address the issues that affect user satisfaction with IT services at each of our facilities. We showed substantial progress between the two surveys, increasing our satisfaction score from 67 to 71. For comparison purposes, our near-term target is to achieve a rating of 75, which would indicate we are in the top half of the ratings for similar organizations globally. VA also uses the ACSI Survey tool to monitor satisfaction with the award winning My Health**e**Vet Personal Health Record portal and our scores in this area (75) benchmark well with the E–Government Index (75).

5. Financial

Finally, we created a detailed financial plan for OI&T in both 2010 and 2011, known as the Prioritized Operating Plan. This plan has two main purposes. First, it creates a vehicle for us to agree, with our customers, on what the high priority IT services and projects are, and allocate our resources to ensure success on the most important items. It also allows us to communicate, clearly and objectively, which projects and services will and will not be accomplished. Second, it allows us to track our expenditures, from plan to budget to spend to results, and know the business purpose for spending each dollar and then track the results we expect to obtain from the expenditure. For 2011, that plan is over 1400 lines long.

VA IT is a Leader in Federal IT

Our efforts in the five focus areas have produced results across the board— results that are seen every day by each of our customers, from a VA employee at a hospital, benefits office, or cemetery, to the Secretary of Veterans Affairs, and to our most important customer, the American Veteran. VA IT is a leader in the Federal Government, and is transforming itself into a 21st Century IT leader by implementing innovative approaches to improve our results.

Our goal is to be the best IT organization in the Federal Government, and comparable to large private-sector organizations. Achieving that goal means being a leader, and being a leader requires more than being good. It requires defining a path in advance of others, and boldly moving forward on that path. To that end, I will highlight a few areas where VA IT is, today, clearly leading the way for the Federal Government.

OMB's 25 point plan

VA has been an early and rapid adopter of the elements of Office of Management and Budget's (OMB) 25 point plan for improving Federal IT. In fact, VA began pursuing many of the initiatives outlined in the 25 point plan while the plan was being formulated. Consequently, VA was uniquely positioned to support the creation of many of the initiatives and become an "early adopter." For example, VA had already begun work on Data Center Consolidation, and was able to provide insight and lessons learned on the process for many other Federal agency participants.

Another initiative in which VA is ahead of the curve is in cloud computing, which we expect to increase efficiency through secure remote access to files and programs.

For example, we have a large-scale, successful cloud program in the Post-9/11 GI Bill, with another starting development for VBMS.

Finally, the VA adapted a key component of our Program Management Accountability System (PMAS), the "strike" meeting to become an early adopter of the program's intervention meetings OMB calls "Techstats." Due to VA's forward thinking, implementation of many of the initiatives outlined in the 25 Point plan was seamless and fit within the plan's structures.

Transparency

VA IT has been a leader in meeting the transparency goals of this administration. One key component of our transparency efforts are the monthly meetings I hold with the staff of the House and Senate Veterans' Affairs Committees. As you know, these meetings serve as an opportunity for VA to inform Congress about IT progress and issues at VA. Through these meetings we have developed a constant dialog that helps keep Congress informed and opens lines of communication.

VA IT is also providing transparency into our development progress. Every increment of every development project is reported in the PMAS Dashboard, which I will discuss in more detail below, which is tied to the OMB dashboard. This gives OMB, Congress, and the public a clear view into VA's IT program management progress.

VA's privacy breach report, discussed below, is another great example of VA's leadership in transparency. Our efforts to present to Congress and the public our data breaches each month has had the effect of limiting the number of breaches that have occurred, and helped our information security staff to better identify potential risks. In addition, the breach report is discussed on a teleconference with the media to ensure an even greater level of transparency.

Shortly after the President's January 21, 2009 Freedom of Information Act (FOIA) Memorandum, VA publicized and implemented the Attorney General's FOIA Guidelines throughout the agency by prominently publishing access links on the VA's FOIA Web site at http://www.foia.va.gov/. VA's Chief Information Officer and VA's Under Secretary for Health appeared in a video directed to all VA FOIA Officers to discuss the importance of FOIA and the implementation of the President's FOIA guidelines by ensuring any releasable items are rapidly made available to the public without requiring a FOIA request. VA has actively improved transparency by routinely posting information about VA Data Breaches. Other offices have also followed the lead and ensured transparency, i.e., VA Office of Finance (OF) posts information regarding VA purchase card holders (credit card) transaction data, First Class and Business Class Travel Reports, VA Civil Service Employee holiday pay data, Unclaimed Moneys Accounts data, VA's FY 2012 President's Budget Submission, and VA's FY 2010 Highlights for the Citizen (Summary of Performance and Financial Information). High level contract award data is also posted without a formal request. VA's ASPIRE for Quality Initiative, a VA-wide program designed to document key measures of health care quality posts outcome information for acute care services, intensive care units, outpatient services, safety and process measures, and indicators of how successful each VA Medical Center has been in meeting its quality goals.

PMAS

In June of 2009, VA introduced the Program Management Accountability System (PMAS). The PMAS process has transformed product delivery at the VA. Before the implementation of PMAS, approximately 283 development projects at VA met their milestone dates an estimated 30 percent of the time. This is an estimate, as IT development projects simply were not tracked to their committed dates prior to PMAS. Today, VA has 107 active development projects, tracked in real-time through a project database and dashboard, that are meeting their milestone dates approximately 75 percent of the time. I know of no other Chief Information Officer (CIO), government or private sector, who has this level of insight into such a large portfolio of development projects. VA is a true trailblazer in product delivery, as I can assure you that most IT development organizations, public or private sector, would be ecstatic with meeting 75 percent of their committed milestones.

PMAS is important for two reasons. Most importantly, we are able to deliver on the transformational capabilities VA requires. PMAS also ensures we meet this administration's goal of ensuring that every taxpayer dollar is well spent. In 2010, VA had a cost avoidance of nearly $200 million by eliminating poorly performing projects and restructuring many others to lower risk, reduce spend rates, and implement incremental development project plans.

PMAS helps VA manage our contracts better by ensuring that proper planning is done prior to beginning development on an increment. That includes having the contracting officer and counsel as part of the Integrated Project Team during the planning phase. During the planning phase of a project, the work is broken into increments that deliver capability to the customer in 6 months or less. As soon as the first increment is planned in sufficient detail, the project can begin development on that increment while continuing to plan future increments. By using PMAS criteria, we ensure that we have good plans and necessary resources in place before a project increment goes active. Once the project is active, it will receive a strike whenever an increment milestone is missed. A project can receive no more than three strikes before it is stopped and forced to re-evaluate the requirement and the plan. While project failures can still occur, we manage the timeline and work so closely that projects cannot fail for years on end before being stopped.

Agile development

A primary driver of our success under PMAS has been the adoption of incremental development. Every project at VA, without exception, must deliver functionality to its users at least every 6 months. Several of our most important projects, including the GI Bill and VBMS, have adopted Agile development methodologies. Whereas PMAS addresses the planning and management aspects of short, incremental delivery, the Agile development methodology provides the technical management guidance of how to turn project requirements into working software quickly and in collaboration with the customer.

Agile development is important to the VA because it encourages continuous input from our customers. In agile projects, all the development priorities are set by the customer, which ensures that the work is performed in the order of importance. To increase the likelihood of success, large projects are broken down into small but valuable increments, each of which could potentially be a candidate for release. This is consistent with our PMAS delivery requirements. Lastly, agile development requires continuous quality assurance throughout the entire development effort, further ensuring high quality deliverables.

Agile software development methodologies are an effective means of improving the predictability, quality, and transparency of software products and their development. At the core of Agile is the iterative work process. Business problems are broken down into small increments of delivery that are tangible products that can be reviewed and verified regularly by business stakeholders. By constantly incorporating feedback, the software that is essential to solving the business problem is created in partnership with stakeholders and any miscommunications, revisions, or changes in business needs can be accommodated quickly and with little rework. The quality of software is kept high throughout the development process as the product in development is kept as close to a production-ready state as possible with each release increment. In addition, prior to the start of each increment, business stakeholders and the development team agree upon which features or requirements are to be satisfied during that increment thus ensuring that the most important work is completed first.

Contrary to popular belief, the successful Agile program requires great rigor as it is essentially a process based on statistical analysis. Every work product (software or otherwise) is defined, broken down and estimated. As work progresses, these work products are carefully tracked on a daily basis and results of progress are published to the team and stakeholders (and any other authorized, interested party) to provide complete transparency. The result of this hyper-transparency is that problems in the development process are identified early and changes, regardless of their origin, can be accommodated quickly and efficiently.

Information Security

To vastly improve our information security posture, we have achieved the goal of providing visibility to every desktop on the network. Visibility to the desktop allows the CIO and our Information Security Team the ability to see, for every machine on the network, what software is installed, whether security policies are met and what vulnerabilities exist—that's more than 314,000 desktops and more than 30,000 laptops reviewed for issues each day. We are easily able to identify outliers and enforce compliance on computers that do not meet our network security requirements.

In our continued effort to further enhance our security posture, we will gain visibility to all servers in the VA environment and implement a strong authentication solution for system administrators by September 2011. In addition to gaining visibility to the server computing domain, VA will take the additional step of gaining

increased visibility of network infrastructure devices. Strong authentication coupled with visibility all the way down to the end user desktop is first-rate for an organization the size of VA and stands to be the one of the largest deployments ever made of security and network management software in a centralized and consolidated network environment. When completed, the VA will have unmatched near real time security situational awareness of its computing resources, consisting of more than three quarters of a million devices.

We have also achieved full implementation of our medical device isolation architecture, which is essential to mitigating security vulnerabilities in our medical devices. The isolation architecture allows us to localize virus outbreaks in populations where providing protection proves more difficult for equipment such as medical devices, by using virtual local area networks and access control lists. These technologies allow us to easily identify threats and vulnerabilities and quarantine them to prevent viruses from spreading across the VA network.

Our achievements on visibility to the desktop and our medical device isolation architecture put us well ahead of most Federal organizations, and on par with well managed private-sector organizations. Our ability to provide immediate response to vulnerabilities and threats within our enterprise, as well as enacting a proactive approach to centralized monitoring, reporting, compliance validation and providing maximum service availability, is quickly establishing VA as a model of excellence for the rest of the Federal Government.

Protecting Personal Private Information

While we have made important strides in reducing the number of data breaches that occur, VA has led the way in both responding to incidents, and providing transparency when reporting data breaches. Our Incident Resolution Team compiles a comprehensive report detailing every reported data breach on a daily and weekly basis. The reports are then discussed with the Data Breach Core Team which is made up of representatives from the Office of General Counsel, Veterans Health Administration, Veterans Benefit Administration, National Cemetery Administration and VA Central Office staff offices. At the end of each month, our Incident Resolution Team compiles a comprehensive report detailing every reported data breach, the circumstances of the breach, the number of Veterans affected, the steps taken to remedy the situation, and any pertinent follow-up information. This information is submitted to Congress, and is also posted publicly on the VA Web site. After its publication, I hold a press conference to discuss the breaches in an open, transparent manner. The number of facilities and the complex IT environments at VA present unique security and privacy challenges. VA's Incident Resolution Team consistently monitors and responds to every privacy or security event, no matter if it deals with one Veteran or thousands. The team members are considered experts in their field, and have assisted other government agencies individually and spoken at Federal IT and privacy events.

VLER

In April 2009, President Obama charged the Secretary of Defense and Secretary of Veterans Affairs to create a Virtual Lifetime Electronic Record (VLER) to bring together the plethora of systems. This was done in order to create a seamless way for servicemembers, Veterans and those who support and care for them to access and manage benefits and care from the day they enter military service and throughout their lives. VLER itself is not a "system", but rather a business and technical redesign initiative that establishes the interoperability and communication environment necessary for DoD, VA and other public and private partners to securely exchange information. The result will improve health, benefits delivery and personnel activities by enabling providers to easily access the information they need. In this way, VLER is enabling health care and benefit providers to proactively deliver the full continuum of services and benefits Veterans have earned through several capability areas that are brought on-line in a measured approach.

The VLER initiative ensures doctrine, policies, organizational structures, personnel training and IT solutions converge to create an environment of information transparency that improves the quality of life for Veterans and servicemembers. The benefits of VLER are already being felt by Veterans and servicemembers around the country in many different ways.

VLER is now being used to support the exchange of health care information between DoD, VA and private health care providers in San Diego, CA; Hampton Roads and Richmond, VA; and Spokane, WA; and Asheville, NC areas. The capability delivered at these pilot sites will become more robust over time and expand to include

six additional regions throughout the country by the end of this fiscal year. In 2012, we will leverage the tools and lessons learned in these 11 areas to provide this clinical encounter support to health care providers who care for Veterans throughout the entire United States.

VLER and the further expansion of the eBenefits portal will empower Veterans and servicemembers by enabling them to access their information, including health care records; benefit applications, benefits information, and other personal information through an interactive web portal. The eBenefits portal is a rapidly growing joint VA/Department of Defense (DoD) service with more than 278,000 registered users as of March 31, 2011. As VLER continues to mature, it will enable the eBenefits portal to provide servicemembers and Veterans more capabilities, including accessing their official military personnel documents, viewing the status of their disability compensation claim, updating direct deposit information for certain benefits, and obtaining a VA guaranteed home loan Certificate of Eligibility. The eBenefits portal effectively bridges the conversion from active duty to Veteran status by allowing servicemembers to retain the same login information they had as an active duty participant. This simple change is critical as it realizes the goal for the VA to be Veteran-centric.

VLER will provide on-line access to all eligibility information, "Notice of Death" reporting, and enhanced support of final honors and memorial benefits under the National Cemetery Administration. Redesign and modernization of cemetery IT systems will include great collaboration with the Department of Defense.

VLER should reduce the cost of the delivery of services, increases efficiency of operations, reduces cycle times for benefits delivery, contributes to the elimination of homelessness, reduces claims backlogs by delivering information sharing capabilities, increases access to benefits by connecting data owners and data users; and, increases the quality and effectiveness of services provided to Veterans and servicemembers. There are certainly obstacles to achieving these lofty goals, but we are optimistic that VLER is making progress to meet the President's vision for the future.

Open Source

The VistA Electronic Health Record (EHR) system is a proven and essential element of VA's ability to provide Veterans with high quality health care and control health care costs. In part because of VistA, VHA has excelled in the last 15 years in both areas. Independent studies have pegged the rate of return on VA's investments in VistA at about $2 returned for every dollar invested.

While the current VistA EHR system meets or exceeds the capabilities currently available from commercial EHR vendors, low investment in VistA over the last decade has eroded its standing from the once-clear clear market leader to being merely competitive. While VA clinicians express strong support and preference for VistA as a clinical tool, they are also vocal and unanimous in calling for us to re-invigorate the innovation that made VistA the best EHR system available.

Clearly, the private sector must play a role in that innovation. The size of private-sector investment and the rate of innovation in the commercial EHR sector far exceeds the government's ability to produce timely, cost-effective EHR products.

VA estimates the cost of replacing VistA with an existing commercial package at $16 billion, based both on VA-commissioned independent validation exercise and on the real-world experiences of Kaiser Permanente. Published reports say that Kaiser spent $4 billion implementing a commercial off-the-shelf EHR system in their 36 hospitals and supporting facilities. Based on size of VA relative to Kaiser (VA has 153 hospitals), $16 billion is a reasonable estimate.

To avoid those costs, and to find a way to involve the private sector in modernizing VistA, the VA is turning to Open Source. Open source software (OSS) began as the "free software" initiative in the early 1980's, though the word free in this context is ambiguous. In this case, it should be thought of as free speech. EHR users from across the community are free to comment and contribute to the evolution of the code base, and VA is free to accept or reject any of those contributions.

In practice, Open Source has proven to be a powerful method of producing production quality software. Market leading products such as Unix, Linux, Netscape, Mozilla, Apache, and many others are the result of Open Source software approaches. And while key product elements such as licensing, cost, security, etc. are different with an Open Source product, they are neither better nor worse. Open source methodologies have been proven many times in high-reliability production environments in the private sector to deliver products that meet or exceed the quality and robustness of proprietary and Government off the Shelf (GOTS) products.

VA has spent more than a year conducting a very deliberative process to examine the implications of Open Source for VistA. We have seen two substantial studies on the topic contributed by the private sector and academia. We have consulted with hundreds of organizations, and thousands of individuals. We have conducted three Requests for Information (RFIs), and received numerous papers, emails, and comments. Our path forward with Open Source has been broadly advised and highly transparent, and is certainly much the better for it.

VA expects that the rate of innovation and improvement in VistA can be increased without increasing our current budget by better involving the private sector (and true private-sector practices) in both the governance and development of the VistA system through Open Source. To that end, we have released a Request for Proposal to establish an Open Source "Custodial Agent," to run the Open Source community. Our estimate of the costs of establishing the Custodial Agent are less than $10 million per year.

Conclusion

Mr. Chairman, over the last 2 years, VA's IT organization has made many significant improvements and had many successes, but there are numerous challenges ahead. We are solidly on the path that we must follow to achieve our ultimate goal of being a leader in Federal IT. But I believe it prudent to reiterate the words from my confirmation testimony that are still true today: "There is no easy path, no simple answer, and no short-cut solution to creating a strong IT capability at VA. Achieving this will require hard work, disciplined management, and honest communications." Mr. Chairman, Ranking Member Donnelly, and Members of this Subcommittee, I am committed to continuing that work. Thank you for your continued support of Veterans, their families and survivors, of VA, and of our efforts to transform VA IT. My colleague and I are prepared to answer any questions you and other Members of the Subcommittee may have.

Prepared Statement of Belinda J. Finn, Assistant Inspector General for Audits and Evaluations, Office of Inspector General, U.S. Department of Veterans Affairs

Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) findings regarding the Department of Veterans Affairs' (VA) management of its information technology (IT) projects. I am accompanied today by Maureen T. Regan, Counselor to the Inspector General.

BACKGROUND

The use of IT is critical to VA providing a range of benefits and services to veterans, from medical care to compensation and pensions. If managed effectively, IT capital investments can significantly enhance operations to support the delivery of VA benefits and services.

However, when VA does not properly plan and manage its IT investments, they can become costly, risky, and counterproductive. As we have reported, IT management at VA is a longstanding high-risk area. Historically, VA has experienced significant challenges in managing its IT investments, including cost overruns, schedule slippages, performance problems, and in some cases, complete project failures. Some of VA's most costly failures have involved management of major IT system development projects awarded to contractor organizations.

IT GOVERNANCE CHALLENGES

In 2009, we provided an overarching view of VA's structure and process for IT investment management (*Audit of VA's Management of Information Technology Capital Investments,* May 29, 2009). As part of the audit, we examined VA's realignment of its IT program from a decentralized to a centralized management structure. The realignment was to provide greater accountability and control over VA resources by centralizing IT operations under the management of the Chief Information Officer (CIO) and standardizing operations using new processes based on industry best practices—goals that have only partially been fulfilled.

We reported that the ad hoc manner in which the Office of Information and Technology (OI&T) managed the realignment inadvertently resulted in an environment with inconsistent management controls and inadequate oversight. Although we conducted this audit more than 2 years after VA centralized its IT program, senior

OI&T officials were still working to develop policies and procedures needed to effectively manage IT investments in a centralized environment. For example, OI&T had not clearly defined the roles of IT governance boards responsible for facilitating budget oversight and IT project management.

Further, in September 2009, we reported that VA needed to better manage its major IT development projects, valued at that time at over $3.4 billion, in a more disciplined and consistent manner (*Audit of VA's System Development Life Cycle Process,* September 30, 2009). In general, we found that VA's System Development Life Cycle (SDLC) processes were adequate and comparable to Federal standards. However, OI&T did not communicate, comply with, or enforce its mandatory software development requirements. OI&T did not ensure that required independent milestone reviews of VA's IT projects were conducted to identify and address system development and implementation issues. Once again, we attributed these management lapses to OI&T centralizing IT operations in an ad hoc manner, leaving little assurance that VA was making appropriate investment decisions and best use of available resources. Moreover, VA increased the risk that its IT projects would not meet cost, schedule, and performance goals, adversely affecting VA's ability to timely and adequately provide veterans health services and benefits.

These audits demonstrated that OI&T needed to implement effective centralized management controls over VA's IT investments. Specifically, we recommended that OI&T develop and issue a directive that communicated the mandatory requirements of VA's SDLC process across the Department. We also recommended that OI&T implement controls to conduct continuous monitoring and enforce disciplined performance and quality reviews of the major programs and projects in VA's IT investment portfolio. Although OI&T concurred with recommendations and provided acceptable plans of actions, OI&T's implementation of the corrective actions is still ongoing. For example, OI&T is reviewing for approval the draft governance board charters and plans to issue a VA directive mandating Program Management Accountability System (PMAS) compliance once version 3.0 of the guide is developed. PMAS is VA's new IT management approach that focuses on achieving schedule objectives while the scope of functionality provided remains flexible.

PROJECT MANAGEMENT SHORTFALLS

Over the past 2 years, our audit work on several IT system development projects has identified themes as to why VA has continued to fall short in its IT project management. These issues include inadequate project and contract management, staffing shortages, lack of guidance, and poor risk management—issues that have repeatedly hindered the success of IT major development projects undertaken by OI&T.

VA's Replacement Scheduling Application

In August 2009, we reported that the Replacement Scheduling Application (RSA) project failed because of ineffective planning and oversight (*Review of the Award and Administration of Task Orders Issued by the Department of Veterans Affairs for the Replacement Scheduling Application Development Program,* August 26, 2009). RSA was a multi-year project to replace the system the Veterans Health Administration used to schedule medical appointments for VA patients. Lacking defined requirements, an IT architecture, and a properly executed acquisition plan, RSA was at significant risk of failure from the start. We suggested that VA needed experienced personnel to plan and manage the development and implementation of complex IT projects effectively. A similar suggestion was made in an earlier report in June 2009, where we noted that VA needed to place greater emphasis on training VA personnel to manage IT enterprise development projects rather than continuing to rely primarily on external organizations and contractors to manage these projects. We believe this condition still exists today and until corrected, VA will struggle to overcome challenges managing its IT investments. *(Review of Interagency Agreement between the Department of Veterans Affairs and Department of Navy, Space and Naval Warfare Systems Center (SPAWAR),* June 4, 2009.) We also suggested that a system to monitor and identify problems affecting the progress of projects could support VA's leadership in making effective and timely decisions to either redirect or terminate troubled projects. PMAS is currently the Department's approach to implementing this suggestion.

Financial and Logistics Integrated Technology Enterprise

In September 2005, VA began developing the Financial and Logistics Integrated Technology Enterprise (FLITE) program to address the longstanding need for an in-

tegrated financial management system. As a successor to the failed Core Financial and Logistics System (CoreFLS), FLITE was a multi-year development effort comprised of three components: an Integrated Financial Accounting System (IFAS), Strategic Asset Management (SAM), and a Data Warehouse. However, as we reported in September 2009, program managers did not fully incorporate lessons learned from the failed CoreFLS program to increase the probability of success in FLITE development (*Audit of FLITE Program Management's Implementation of Lessons Learned,* September 16, 2009). For example, critical FLITE program functions were not fully staffed, non-FLITE expenditures were improperly funded through the FLITE program, and contract awards did not comply with competition requirements. We recommended that FLITE program managers develop written procedures to manage and monitor lessons learned and expedite actions to ensure full staffing of the FLITE program.

Audit of the FLITE Strategic Asset Management Pilot Project

Our report on the SAM pilot project disclosed that FLITE program managers did not take well-timed actions to ensure VA achieved cost, schedule, and performance goals. Further, the contractor did not provide acceptable deliverables in a timely manner (*Audit of the FLITE Strategic Asset Management Pilot Project,* September 14, 2010). Once again, we identified instances where FLITE program managers could have avoided mistakes by paying closer attention to lessons learned from the CoreFLS effort.

Specifically, FLITE program managers:

- Awarded a task order on April 21, 2009, to General Dynamics for implementation of the SAM pilot project, even though the FLITE program suffered from a known shortage of legacy system programmers critical to integration efforts required to make FLITE a success.
- Did not clearly define FLITE program and SAM pilot project roles and responsibilities, resulting in confusion and unclear communications between VA and General Dynamics. Contractor personnel indicated that they received directions and guidance from multiple sources. One of their biggest obstacles was trying to overcome the lack of one clear voice for VA's FLITE program.
- Did not ensure that the solicitation for the SAM pilot project clearly described VA's requirements for SAM end-user training. As such, VA contractually agreed to a training solution that did not meet its expectations. General Dynamics subsequently revised its training approach to meet VA's needs, but at a total cost of $1,090,175, which was more than a 300 percent increase from the original $244,451 training cost.
- Did not always effectively identify and manage risks associated with the SAM pilot project even though inadequate risk management had also been a problem with the failed CoreFLS. Specifically, FLITE program managers did not take steps early on to ensure that the contractor participated in the risk management process and that the Risk Control Review Board adequately mitigated risks before closing them.

Because of such issues, in early 2010 VA was considering extending the SAM pilot project by 17 months (from 12 to 29 months), potentially more than doubling the original contract cost of $8 million. We recommended that VA establish stronger program management controls to facilitate achieving cost, schedule, and performance goals, as well as mitigating risks related to the successful accomplishment of the SAM pilot project. (SAM was suspended in March 2011 for not meeting user requirements. Further details are discussed below.)

Review of Alleged Improper Program Management within the FLITE Strategic Asset Management Pilot Project

This report, in response to a hotline allegation, disclosed that FLITE program managers needed to improve their overall management of the SAM pilot project (*Review of Alleged Improper Program Management within the FLITE Strategic Asset Management Pilot Project,* September 7, 2010). FLITE program managers did not develop written procedures that clearly defined roles and responsibilities, provide timely guidance to program and contract staff, or foster an effective working environment within the FLITE program. FLITE program managers also did not ensure certain elements considered necessary for a successful software development effort, such as "to be" and architectural models were included as project deliverables in the FLITE program. In general, we recommended that VA strengthen project management controls to improve the SAM pilot, beta, and national deployment projects.

New Office of Management and Budget (OMB) guidance on financial systems IT projects, issued on June 28, 2010, also had a major impact on the FLITE program. OMB issued the guidance because large-scale financial system modernization efforts undertaken by Federal agencies have historically led to complex project management requirements that are difficult to manage. Moreover, by the time the lengthy projects are finished, they are technologically obsolete. Consequently, OMB directed all Chief Financial Officer Act agencies immediately to halt the issuance of new procurements for financial system projects until it approves new project plans developed by the agencies. In July 2010, VA's Assistant Secretary for Information and Technology announced termination of the IFAS and Data Warehouse portions of FLITE. In March 2011, the SAM pilot project, the final component of the FLITE program, was suspended just weeks before it was scheduled for deployment. SAM had received its "third strike" in the PMAS review process for failing user acceptance testing, which indicated that SAM was not ready for live operation. As of March 2011, program managers estimated obligations of about $126 million for the FLITE program; of that amount, the SAM project represented approximately $40 million.

GI Bill Long Term Solution

In September 2010, we reported that OI&T's plan for deployment of the GI Bill Long Term Solution (LTS) was effective in part (*Audit of VA's Implementation of the Post-9/11 GI Bill Long Term Solution,* September 30, 2010). LTS is a fully automated claims processing system that utilizes a rules-based engine to process Post-9/11 GI Bill Chapter 33 veterans' education benefits.

OI&T developed and deployed both LTS Releases 1 and 2 on time. Lacking the management discipline and processes necessary to control performance and cost in project development, OI&T has relied upon PMAS to achieve project scheduling goals. With this schedule-driven strategy, OI&T has been able to satisfy users and incrementally move VA forward in providing automated support for education benefits processing under the Post-9/11 GI Bill.

However, OI&T's achievement of the time frames for LTS Releases 1 and 2 required that VA sacrifice much of the system functionality promised. Specifically, due to unanticipated complexities in developing the system, OI&T deployed Release 1 as a "pilot" to approximately 16 claims examiners, with the functionality to handle only 15 percent of the Chapter 33 education claims that the Veterans Benefits Administration anticipated processing. Release 2 caught up on the functionality postponed from Release 1, while providing the capability to process 95 percent of all Chapter 33 education claims. However, due to data structure and quality issues that still had to be overcome, users could not make use of all of the functionality provided through Release 2 and were able to process only 30 percent of all Chapter 33 education claims. In addition to these performance issues, OI&T did not have processes in place to track actual LTS project costs.

Following Release 3 that allowed VA to automate input of college enrollment information, OI&T deployed LTS Release 4 in accordance with the original delivery schedule of December 2010. OI&T recently deployed LTS Release 4.2 and has plans for two additional releases, tentatively scheduled for June and November 2011, to accommodate recent revisions to the Post-9/11 GI Bill. These LTS releases should provide enhancements such as automated scheduling for future housing allocations, and claims processing for licensing and certification and national tests. Any delays in providing the promised functionality could require continued manual processing, which could in turn delay payment of GI Bill benefits to veterans.

In the absence of effective performance and cost controls, OI&T runs the risk that future LTS releases may continue to meet schedule, but at the expense of performance and cost project goals. We recommended that OI&T improve LTS management by conducting periodic independent reviews to help identify and address system development and implementation issues as they arise. We also recommended that OI&T adopt cost control processes and tools to ensure accountability for LTS costs in accordance with Federal IT investment management requirements. OI&T concurred with our recommendations and provided acceptable plans of action, but implementation of corrective actions such as putting independent oversight reviews into place is still ongoing.

Veterans Services Network

In February 2011, we reported that the Veterans Services Network (VETSNET) program faces the continuing challenge of managing competing requirements and new systems initiatives that have repeatedly changed the scope and direction of the

program (*Audit of the Veterans Service Network,* **February 11, 2001).** Since 1996, VA has been working on this effort to consolidate compensation and pension benefits processing into a single replacement system. However, the repeated changes have adversely impacted schedule, cost, and performance goals over the life of VETSNET development. Given a loss of focus concerning the end goals of the program, VA's plans and time frames for retiring the aging Benefits Delivery Network and migrating all entitlement programs to the VETSNET Corporate Database have become unclear. Work to meet original program objectives has been extended by nearly 5 years. In 2009, VA reported a revised cost estimate of $308 million through 2012, more than two times an amount previously projected in 2006.

Further, frequently changing business requirements have necessitated additional VETSNET software releases. Because software change controls and testing have not been adequate to ensure proper system functionality, software rework and rollback of installation packages have been required to correct defects, and planned functionality enhancements have been delayed. We recommended that VA align resources and establish a schedule for accomplishing the original goals of VETSNET in the near term. We also recommended that VA implement improved processes to address software development deficiencies.

IT ACQUISITION AND CONTRACT MANAGEMENT WEAKNESSES

In response to a hotline complaint, we reviewed the contract awarded to Catapult Technology, Ltd., for the installation of wireless fidelity (Wi-Fi) services at 236 VA sites (*Review of Allegations of Acquisition Planning Weaknesses and Cost Overruns on the Contract Awarded to Catapult Technology, Ltd.,* March 31, 2011). The complainant made several allegations regarding the award and administration of the contract. Our review substantiated all of the allegations except one, and partially substantiated the remaining allegation.

We determined that the time frames established to plan, solicit, and award the contract were unreasonable. VA did not establish firm requirements and issued a Statement of Objectives that lacked the detail needed for vendors to submit reasonable, firm fixed-price proposals. Because of inadequate planning and incomplete information regarding requirements, VA processed modifications that caused contract costs to increase significantly; the current contract costs are projected at $161.5 million, which is a $70.5 million (77 percent) increase in contract costs.

VA processed modifications adding additional sites; however, the contract had no provision that permitted VA to increase the number of sites. We also determined that VA was improperly paying Catapult on a milestone basis rather than on a completed site basis according to the contract terms. This was not only inconsistent with the contract, it was also inconsistent with the information provided to vendors during solicitation. The Office of Acquisitions and Logistics concurred with all our findings and recommendations and terminated the contract.

CONCLUSION

VA continues to rely on IT advancements to provide better services to our Nation's veterans. Historically, VA has struggled to manage IT developments that successfully deliver desired results within cost, schedule, and performance objectives. OI&T recently implemented PMAS to strengthen IT project management and improve the rate of success of VA's IT projects. We are currently conducting an audit to determine whether OI&T has planned and implemented PMAS with the management controls needed for effective oversight of the Department's IT initiatives. Specifically, we are examining PMAS data reliability, project cost tracking, and guidance and processes for ensuring project compliance with the oversight approach. Our audit results should provide valuable information to VA and Congress as VA moves forward in managing its technology investments. We expect to issue a final report this summer.

Mr. Chairman, this concludes my statement. We would be pleased to answer any questions that you or other Members of the Subcommittee may have.

Prepared Statement of Joel C. Willemssen, Managing Director, Information Technology, U.S. Government Accountability Office

INFORMATION TECHNOLOGY: Department of Veterans Affairs Faces Ongoing Management Challenges

GAO HIGHLIGHTS

Why GAO Did This Study

The use of information technology (IT) is crucial to helping the Department of Veterans Affairs (VA) effectively serve the Nation's veterans, and the department has expended billions of dollars annually over the last several years to manage and secure its information systems and assets. VA has, however, experienced challenges in managing its IT. GAO has previously highlighted VA's weaknesses in managing and securing its information systems and assets.

GAO was asked to testify on its past work on VA's weaknesses in managing its IT resources, specifically in the areas of systems development, information security, and collaboration with the Department of Defense (DoD) on efforts to meet common health system needs.

What GAO Recommends

In previous reports in recent years, GAO has made numerous recommendations to VA aimed at improving the department's IT management capabilities. These recommendations were focused on: improving two projects to develop and implement new systems, strengthening information security practices and ensuring that security issues are adequately addressed, and overcoming barriers VA faces in collaborating with DoD to jointly address the departments' common health care business needs.

What GAO Found

Recently, GAO reported on two VA systems development projects that have yielded mixed results. For its outpatient appointment scheduling project, VA spent an estimated $127 million over 9 years and was unable to implement any of the planned capabilities. The application software project was hindered by weaknesses in several key management disciplines, including acquisition planning, requirements analysis, testing, progress reporting, risk management, and oversight. For its Post-9/11 GI Bill educational benefits system, VA used a new incremental software development approach and deployed the first two of four releases of its long-term system solution by its planned dates, thereby providing regional processing offices with key automated capabilities to prepare original and amended benefits claims. However, VA had areas for improvement, including establishing business priorities, testing the new systems, and providing oversight.

Effective information security controls are essential to securing the information systems and information on which VA depends to carry out its mission. For over a decade, VA has faced long-standing information security weaknesses as identified by GAO, VA's Office of the Inspector General, VA's independent auditor, and the department itself. The department continues to face challenges in maintaining its information security controls over its systems and in fully implementing the information security program required under the Federal Information Security Management Act of 2002. These weaknesses have left VA vulnerable to disruptions in critical operations, theft, fraud, and inappropriate disclosure of sensitive information.

VA and DoD operate two of the Nation's largest health care systems, providing health care to 6 million veterans and 9.6 million active duty servicemembers at estimated annual costs of about $48 billion and $49 billion, respectively. To provide this care, both departments rely on electronic health record systems to create, maintain, and manage patient health information. GAO reported earlier this year that VA faced barriers in establishing shared electronic health record capabilities with DoD in three key IT management areas—strategic planning, enterprise architecture (i.e., a description of business processes and supporting technologies), and IT investment management. Specifically, the departments were unable to articulate explicit plans, goals, and time frames for jointly addressing the health IT requirements common to both departments' electronic health record systems. Additionally, although VA and DoD took steps toward developing and maintaining artifacts related to a joint health architecture, the architecture was not sufficiently mature to guide the departments' joint health IT modernization efforts. Lastly, VA and DoD did not have a joint process for selecting IT investments based on criteria that consider cost, ben-

efit, schedule, and risk elements, which would help to ensure that the chosen solution both meets the departments' common health IT needs and provides better value and benefits to the government as a whole. Subsequent to our report, the Secretaries of Veterans Affairs and Defense agreed to pursue integrated electronic health record capabilities.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be a part of today's dialogue with the Subcommittee on the Department of Veterans Affairs' (VA) actions to better manage its information technology (IT) resources. The use of IT is crucial to helping VA effectively serve the Nation's veterans and the department has expended billions of dollars over the last several years to manage and secure its information systems and assets—the department's budget for IT now exceeds $3 billion annually.

VA has, however, experienced challenges in managing its IT resources, as we have previously reported.[1] As you requested, in my testimony today, I will describe those challenges, specifically in the areas of systems development, information security, and collaborating with the Department of Defense (DoD) to jointly develop electronic health record system capabilities.

The information in my testimony is based primarily on our previous work at VA. We also obtained and analyzed pertinent documentation to determine the current status of selected department management efforts. We conducted our work in support of this testimony during May 2011 in the Washington, D.C., area. All work on which this testimony is based was conducted in accordance with generally accepted government auditing standards.

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. According to information from the department, its employees maintain the largest integrated health care system in the Nation for more than 5 million patients at more than 1,500 sites of care, provide compensation and pension benefits for nearly 4 million veterans and beneficiaries, and maintain nearly 3 million gravesites at 163 properties. Over time, the use of IT has become increasingly important to the department's efforts to provide these benefits and services to veterans; VA relies on its IT systems for medical information and records and for processing benefits claims, including compensation and pension and education benefits. Further, VA is increasingly expected to improve its service to veterans by sharing information with other departments, especially DoD.

VA's fiscal year 2012 request for almost $3.2 billion in IT budget authority indicates the range of the department's IT activities. For example, the request includes:

- about $1.4 billion to operate and maintain existing infrastructure and systems;
- approximately $650 million to develop new system capabilities to support, for example, faster compensation and pension claims processing, elimination of veteran homelessness, and improvement of veteran mental health;
- $68 million for information security activities; and
- $915 million to fund about 7,000 IT personnel.

Our prior work has shown that success in managing IT depends, among other things, on having and using effective system development capabilities and having effective controls over information and systems. We have issued several products on VA in important management areas where the department faces challenges. My testimony today will briefly summarize these products.

---

[1] GAO, *Electronic Health Records: DoD and VA Should Remove Barriers and Improve Efforts to Meet Their Common System Needs,* GAO–11–265 (Washington, D.C.: February 2011); *Information Technology: Veterans Affairs Can Further Improve Its Development Process for Its New Education Benefits System,* GAO–11–115 (Washington, D.C.: December 2010); *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing,* GAO–10–513 (Washington, D.C.: May 2010); *Information Technology: Management Improvements Are Essential to VA's Second Effort to Replace Its Outpatient Scheduling System,* GAO–10–579 (Washington, D.C.: May 2010); and *Information Security: Veterans Affairs Needs to Resolve Long-Standing Weaknesses,* GAO–10–727T (Washington, D.C.: May 19, 2010).

Recent System Development Projects Have Achieved Varied Degrees of Success

Historically, VA has experienced significant IT development and delivery difficulties. We recently reported on two important VA systems development projects.[2] The first project expended an estimated $127 million without delivering any of the planned capabilities. VA has begun implementing capabilities from the second project, although we identified opportunities for improvement.

VA's Scheduling Replacement Project Was Hindered by Systems Development and Acquisition Weaknesses

To carry out VA's daily operations in providing care to veterans and their families, the department relies on an outpatient appointment scheduling system. However, according to the department, this current scheduling system has had longstanding limitations that have impeded its effectiveness. Consequently, VA began work on a replacement system in 2000. However, after spending an estimated $127 million over 9 years, VA had not implemented any of the planned capabilities.

VA's efforts to successfully complete the Scheduling Replacement Project were hindered by weaknesses in several key project management disciplines and a lack of effective oversight. Specifically,

- **VA did not adequately plan its acquisition of the scheduling application and did not obtain the benefits of competition.** The *Federal Acquisition Regulation* (FAR) required preparation of acquisition plans[3] that must address how competition will be sought, promoted, and sustained.[4] VA did not develop an acquisition plan until May 2005, about 4 years after the department first contracted for a new scheduling system. Further, VA did not promote competition in contracting for its scheduling system. Instead, VA issued task orders against an existing contract that the department had in place for acquiring services such as printing, computer maintenance, and data entry. These weaknesses in VA's acquisition management reflected the inexperience of the department's personnel in administering major IT contracts. To address identified shortcomings, we recommended that VA ensure that future acquisition plans document how competition will be sought, promoted, and sustained.
- **VA did not ensure that requirements were complete and sufficiently detailed.** Effective, disciplined practices for defining requirements include analyzing requirements to ensure that they are complete, verifiable, and sufficiently detailed.[5] For example, maintaining bidirectional traceability from high-level operational requirements through detailed low-level requirements to test cases is a disciplined requirements management practice. However, VA did not adequately define requirements. For example, in November 2007, VA determined that performance requirements were missing and that some requirements were not testable. Further, according to project officials, some requirements were vague and open to interpretation. Also, requirements for processing information from other systems were missing. The incomplete and insufficiently detailed requirements resulted in a system that did not function as intended. In addition, VA did not ensure that requirements were fully traceable. As early as October 2006, an internal review noted that the requirements did not trace to business rules or to test cases. By not ensuring requirements traceability, the department increased the risk that the system could not be adequately tested and would not function as intended. We therefore recommended that VA ensure implementation of a requirements management plan that reflected leading practices.
- **VA's concurrent approach to performing system tests increased risk.** Best practices in system testing indicate that testing activities should be performed incrementally, so that problems and defects[6] with software versions can be discovered and corrected early. VA's guidance on conducting tests is

[2] GAO–10–579 and GAO–11–115.

[3] See FAR, subpart 7.1. See also FAR 34.004.

[4] See FAR 7.105 b(2).

[5] See Carnegie Mellon Software Engineering Institute, *Capability Maturity Model*® Integration for Development, version 1.2 (Pittsburgh, Pa., August 2006), and *Software Acquisition Capability Maturity Model (SA–CMM) version 1.03,* CMU/SEI–2002–TR–010 (Pittsburgh, Pa., March 2002).

[6] Defects are system problems that require a resolution and can be due to a failure to meet the system specifications.

consistent with these practices and specifies four test stages and associated criteria for progressing through the stages.[7] For example, defects categorized as critical, major, and average severity identified in testing stage one are to be resolved before testing in stage two is begun. Nonetheless, VA took a high-risk approach to testing by performing tests concurrently rather than incrementally. Scheduling project officials told us that they ignored their own testing guidance and performed concurrent testing at the direction of Office of Enterprise Development senior management in an effort to prevent project timelines from slipping. The first version to undergo stage two testing had 370 defects that should have been resolved before stage two testing was begun. Almost 2 years after beginning stage two testing, 87 defects that should have been resolved before stage two testing began had not been fixed. As a result of a large number of defects that VA and the contractor could not resolve, the contract was terminated. To prevent these types of problems with future system development efforts, we recommended that VA adhere to its own guidance for system testing.

- **VA's reporting based on earned value management data was unreliable.** The Office of Management and Budget (OMB) and VA policies require major projects to use earned value management[8] to measure and report progress. Earned value management is a tool for measuring a project's progress by comparing the value of work accomplished with the amount of work expected to be accomplished. Such a comparison permits actual performance to be evaluated and is based on variances[9] from the cost and schedule baselines. In January 2006, the scheduling project began providing monthly reports to the department's Chief Information Officer based on earned value management data. However, the progress reports included contradictory information about project performance. Specifically, the reports featured stoplight indicators (green, yellow, or red) that frequently were inconsistent with the reports' narrative. For example, the June 2007 report identified project cost and schedule performance as green, despite the report noting that the project budget was being increased by $3 million to accommodate schedule delays. This inconsistent reporting continued until October 2008, when the report began to show cost and schedule performance as red, the actual state of the project. Further, the former program manager noted that the department performed earned value management for the scheduling project only to fulfill the OMB requirement, and that the data were not used as the basis for decision-making because doing so was not a part of the department's culture. To address these weaknesses, we recommended that VA ensure effective implementation of earned value management.
- **VA did not effectively identify, mitigate, and communicate project risks.** Federal guidance and best practices advocate risk management.[10] To be effective, risk management activities should include identifying and prioritizing risks as to their probability of occurrence and impact, documenting them in an inventory, and developing and implementing appropriate risk mitigation strategies. VA established a process for managing the scheduling system project's risks that was consistent with relevant best practices. Specifically, project officials developed a risk management plan that defined five phases—risk identification, risk analysis, risk response planning, risk monitoring and control, and risk review. However, the department did not take key project risks into account. Senior project officials indicated that staff members were often reluctant to raise risks or issues to leadership due to the emphasis on keeping the project on schedule. Accordingly, VA did not identify as risks (1) using a noncompetitive acquisition approach, (2) conducting concurrent testing and initiation of stage two testing with significant defects, and (3) reporting unreliable project cost and schedule performance information.

---

[7] According to VA testing documentation, these stages are (1) testing within the VA development team, (2) testing services, (3) field testing, and (4) final review and acceptance testing.

[8] OMB issued policy guidance (M–05–23) to agency CIOs on improving technology projects that includes requirements for reporting performance to OMB using earned value management (August 2005).

[9] Cost variances compare the value of the completed work (i.e., the earned value) with the actual cost of the work performed. Schedule variances are also measured in dollars, but they compare the earned value of the completed work with the value of the work that was expected to be completed. Positive variances indicate that activities cost less or are completed ahead of schedule. Negative variances indicate activities cost more or are falling behind schedule.

[10] OMB Circular A–130 (Nov. 30, 2000) and Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration for Development,* version 1.2 (Pittsburgh, Pa., August 2006).

Any one of these risks alone had the potential to adversely impact the outcome of the project. The three of them together dramatically increased the likelihood that the project would not succeed. To improve management of the project moving forward, we recommended that VA identify risks related to the scheduling project and prepare plans and strategies to mitigate them.

- **VA's oversight boards did not take corrective actions despite the department becoming aware of significant issues.** GAO and OMB guidance call for the use of institutional management processes to control and oversee IT investments.[11] Critical to these processes are milestone reviews that include mechanisms to identify underperforming projects, so that timely steps can be taken to address deficiencies. These reviews should be conducted by a department-level investment review board composed of senior executives. In this regard, VA's Enterprise Information Board was established to provide oversight of IT projects through in-process reviews when projects experience problems. Similarly, the Programming and Long-Term Issues Board is responsible for performing milestone reviews and program management reviews of projects. However, between June 2006 and May 2008, the department did not provide oversight of the Scheduling Replacement Project, even though the department had become aware that the project was having difficulty meeting its schedule and performance goals. According to the chairman of the Programming and Long-Term Issues Board, it did not conduct reviews of the scheduling project prior to June 2008 because it was focused on developing the department's IT budget strategy. To address these deficiencies, in June 2009, VA began establishing the Program Management Accountability System to promote visibility into troubled programs and allow the department to take corrective actions. We recommended that VA ensure the policies and procedures it was establishing were executed effectively.

In response to our report, VA concurred with our recommendations and described its actions to address them. For example, the department stated that it would work closely with contracting officers to ensure future acquisition plans clearly identify an acquisition strategy that promotes full and open competition. In addition, the department stated that the Program Management Accountability System will provide near-term visibility into troubled programs, allowing the Principal Deputy Assistant Secretary for Information and Technology to provide help earlier and avoid long-term project failures.

In May 2011, VA's program manager stated that the department's effort to develop a new outpatient scheduling system—now referred to as 21st Century Medical Scheduling—consists largely of planning activities, including the identification of requirements. However, according to the manager, the project is not included in the department's fiscal year 2012 budget request. As a result, the department's plans for addressing the limitations that it had identified in its current scheduling system are uncertain.

VA Has Partially Delivered New Education Benefits System Capabilities, but Can Improve Its Development Process

In contrast to the scheduling system project failure, VA has begun implementing a new system for processing a recently established education benefit for veterans. The Post-9/11 GI Bill provides educational assistance for veterans and members of the armed forces who served on or after September 11, 2001. VA concluded that its existing system and manual processes were insufficient to support the new benefits. For instance, the system was not fully integrated with other information systems such as VA's payments system, requiring claims examiners to access as many as six different systems and manually input claims data. Consequently, claims examiners reportedly took up to six times longer to pay Post-9/11 GI Bill program claims than other VA education benefit claims. The challenges associated with its processing system contributed to a backlog of 51,000 claims in December 2009. In response to this situation, the department began an initiative to modernize its benefits processing capabilities. VA chose an incremental development approach, referred to as Agile software development,[12] which is intended to deliver functionality in short increments before the system is fully deployed.

---

[11] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity,* GAO–04–394G (Washington, D.C.: March 2004) and OMB, *Capital Programming Guide: Supplement to Circular A–11, Part 7, Planning, Budgeting, and Acquisition of Capital Assets* (Washington, D.C., June 2006).

[12] Agile software development is not a set of tools or a single methodology, but a philosophy based on selected values, such as, the highest priority is to satisfy customers through early and

In December 2010, we reported that VA had delivered key automated capabilities used to process the new education benefits. Specifically, it deployed the first two of four releases of its long-term system solution by its planned dates, thereby providing regional processing offices with key automated capabilities to prepare original and amended benefits claims. Further, VA established Agile practices including a cross-functional team that involves senior management, governance boards, key stakeholders, and distinct Agile roles and began using three other Agile practices—focusing on business priorities, delivering functionality in short increments, and inspecting and adapting the project.

However, to help guide the full development and implementation of the new system, we reported that VA could make further improvements to these practices in five areas.

1. **Business priorities.** To ensure business priorities are a focus, a project starts with a vision that contains, among other things, a purpose, goals, metrics, and constraints. In addition, it should be traceable to requirements. VA established a vision that captured the project purpose and goals; however, it had not established metrics for the project's goals or prioritized project constraints. Department officials stated that project documentation was evolving and they intended to improve their processes based on lessons learned; however, until it identified metrics and constraints, the department did not have the means to compare the projected performance with the actual results. We recommended that VA establish performance measures for goals and identify constraints to provide better clarity in the vision and expectations of the project.
2. **Traceability.** VA had also established a plan that identified how to maintain requirements traceability within an Agile environment; however, the traceability was not always maintained between legislation, policy, business rules, and test cases. We recommended that VA establish bidirectional traceability between requirements and legislation, policies, and business rules.
3. **Definition of "done."** To aid in delivering functionality in short increments, defining what constitutes completed work and testing functionality is critical.[13] However, VA had not established criteria for work that was considered "done" at all levels of the project. Program officials stated that each development team had its own definition of "done" and agreed that they needed to provide a standard definition across all teams. Without a mutual agreement for what constitutes "done" at each level, the resulting confusion can lead to inconsistent quality. We therefore recommended that VA define the conditions that must be present to consider work "done" in adherence with agency policy and guidance.
4. **Testing.** While the department had established an incremental testing approach, the quality of unit and functional testing performed during Release 2 was inadequate in 10 of the 20 segments of system functionality we reviewed. Program officials stated that they placed higher priority on user acceptance testing at the end of a release and relied on users to identify defects that were not detected during unit and functional testing. Without improved testing quality, the department risks deploying future releases that contain defects that may require rework. To reduce defects and rework to fix them, we recommended that VA improve the adequacy of the unit and functional testing processes.
5. **Oversight.** In order for projects to be effectively inspected and adapted, management must have tools to provide effective oversight. For Agile development, progress and the amount of work remaining can be reflected in a burn-down chart, which depicts how factors such as the rate at which work is completed (velocity) and changes in overall product scope affect the project over time. While VA had an oversight tool that showed the percentage of work completed to reflect project status at the end of each iteration, it did not depict the velocity of the work completed and the changes to scope over time. We therefore recommended that VA implement an oversight tool to clearly communicate velocity and the changes to project scope over time.

---

continuous delivery of valuable software; delivering working software frequently, from a couple of weeks to a couple of months; and that working software is the primary measure of progress. For more information on Agile development, see http://www.agilealliance.org.

[13] One of the key Agile principles is that the delivery of completed software be defined, commonly referred to as the definition of "done." This is critical to the development process to help ensure that, among other things, testing has been adequately performed and the required documentation has been developed.

VA concurred with three of our five recommendations. It did not concur with our recommendation that it implement an oversight tool to clearly communicate velocity. However, without this level of visibility in its reporting, management and the development teams may not have all the information they need to fully understand project status. VA also did not concur with our recommendation to improve the adequacy of the unit and functional testing processes to reduce the amount of system rework. However, without increased focus on the quality of testing early in the development process, VA risks delaying functionality and/or deploying functionality with unknown defects that could require future rework that may be costly and ultimately impede the claims examiners' ability to process claims efficiently.

In early May 2011, we reported that the implementation of remaining capabilities is behind schedule and additional modifications are needed.[14] According to VA officials, system enhancements such as automatic verification of the length of service were delayed because of complexities with systems integration and converting data from the interim system. Additionally, recent legislative changes to the program required VA to modify the system and its deployment schedule. For instance, VA will need to modify its system to reflect changes to the way tuition and fees are calculated—an enhancement that officials described as difficult to implement. Because of these delays, final deployment of the system is now scheduled for the end of 2011—a year later than planned.

VA Continues To Face Information Security Challenges

Effective information security controls[15] are essential to securing the information systems and information on which VA depends to carry out its mission. Without proper safeguards, the department's systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The consequence of weak information security controls was illustrated by VA's May 2006 announcement that computer equipment containing personal information on veterans and active duty military personnel had been stolen. Further, over the last few years, VA has reported an increasing number of security incidents and events. Specifically, each year during fiscal years 2007 through 2009, the department reported a higher number of incidents and the highest number of incidents in comparison to 23 other major Federal agencies.

To help protect against threats to Federal systems, the Federal Information Security Management Act of 2002 (FISMA) sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. The framework creates a cycle of risk management activities necessary for an effective security program. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to OMB, agency heads, chief information officers, inspectors general, and the National Institute of Standards and Technology (NIST), in particular requiring chief information officers and inspectors general to submit annual reports to OMB.

In addition, Congress enacted the Veterans Benefits, Health Care, and Information Technology Act of 2006.[16] Under the act, VA's Chief Information Officer is responsible for establishing, maintaining, and monitoring departmentwide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department's information security program. It also reinforced the need for VA to establish and carry out the responsibilities outlined in FISMA, and included provisions to further protect veterans and servicemembers from the misuse of their sensitive personal information and to inform Congress regarding security incidents involving the loss of that information.

---

[14] GAO, *Veterans' Education Benefits: Enhanced Guidance and Collaboration Could Improve Administration of the Post-9/11 GI Bill Program,* GAO–11–356R (Washington, D.C.: May 2011).

[15] Information system general controls affect the overall effectiveness and security of computer operations and are not unique to specific computer applications. These controls include security management, configuration management, operating procedures, software security features, and physical protections designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that incompatible computer-related duties are segregated, and that backup and recovery plans are adequate to ensure the continuity of operations.

[16] *Veterans Benefits, Health Care, and Information Technology Act of 2006,* Pub. L. No. 109–461, 120 Stat. 3403, 3450 (Dec. 22, 2006).

Weaknesses in Security Controls Have Placed VA's Systems at Risk

Information security has been a long-standing challenge for the department, as we have previously reported. In 2010, for the 14th year in a row, VA's independent auditor reported that inadequate information system controls over financial systems constituted a material weakness.[17] Among 24 major Federal agencies, VA was one of eight agencies in fiscal year 2010 to report such a material weakness.

VA's independent auditor stated that, while the department continued to make steady progress, IT security and control weaknesses remained pervasive and placed VA's program and financial data at risk. The auditor noted the following weaknesses:

- Passwords for key VA network domains and financial applications were not consistently configured to comply with agency policy.
- Testing of contingency plans for financial management systems at selected facilities was not routinely performed and documented to meet the requirements of VA policy.
- Many IT security control deficiencies were not analyzed and remediated across the agency and a large backlog of deficiencies remained in the VA plan of action and milestones system. In addition, previous plans of action and milestones were closed without sufficient and documented support for the closure.

In addition, VA has consistently had weaknesses in major information security control areas. As shown in table 1, for fiscal years 2007 through 2010, deficiencies were reported in each of the five major categories of information security access controls [18] as defined in our *Federal Information System Controls Audit Manual.*[19]

Table 1: Control Weaknesses for Fiscal Years 2007–2010

Security control category	2007	2008	2009	2010
Access control	•	•	•	•
Configuration management	•	•	•	•
Segregation of duties	•	•	•	•
Contingency planning	•	•	•	•
Security management	•	•	•	•

Source: GAO analysis based on VA and Inspector General reports.

In fiscal year 2010, for the 11th year in a row, the VA's Office of Inspector General designated VA's information security program and system security controls as a major management challenge for the department. Of 24 major Federal agencies, the department was 1 of 23 to have information security designated as a major management challenge. The Office of Inspector General noted that the department had made progress in implementing components of an agencywide information security program, but nevertheless continued to identify major IT security deficiencies in the annual information security program audits. To assist the department in improving its information security, the Office of Inspector General made recommendations for strengthening access controls, configuration management, change management, and service continuity. Effective implementation of these recommendations could help VA to prevent, limit, and detect unauthorized access to computerized net-

[17] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

[18] Access controls ensure that only authorized individuals can read, alter, or delete data; configuration management controls provide assurance that only authorized software programs are implemented; segregation of duties reduces the risk that one individual can independently perform inappropriate actions without detection; continuity of operations planning provides for the prevention of significant disruptions of computer-dependent operations; and an agencywide information security program provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

[19] GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO–09–232G (Washington, D.C.: Feb. 2009).

works and systems and help ensure that only authorized individuals can read, alter, or delete data.

In March 2010, we reported [20] that Federal agencies, including VA, had made limited progress in implementing the Federal Desktop Core Configuration (FDCC) initiative to standardize settings on workstations.[21] We determined that VA had implemented certain requirements of the initiative, such as documenting deviations from the standardized set of configuration settings for Windows workstations and putting a policy in place to officially approve these deviations. However, VA had not fully implemented several key requirements. For example, the department had not included language in contracts to ensure that new acquisitions address the settings and that products of IT providers operate effectively using them. Additionally, VA had not obtained a NIST-validated tool to monitor implementation of standardized workstation configuration settings. To improve the department's implementation of the initiative, we made four recommendations: (1) complete implementation of VA's baseline set of configuration settings, (2) acquire and deploy a tool to monitor compliance with FDCC, (3) develop, document, and implement a policy to monitor compliance, and (4) ensure that FDCC settings are included in new acquisitions and that products operate effectively using these settings. VA concurred and has addressed the recommendation to ensure settings are included in new acquisitions. The department intends to implement the remaining recommendations in the future.

VA's Uneven Implementation of FISMA Has Limited the Effectiveness of Security Efforts

FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As part of its oversight responsibilities, OMB requires agencies to report on specific performance measures, including the percentage of:

- employees and contractors receiving IT security awareness training and those who have significant security responsibilities and have received specialized security training,
- systems whose controls were tested and evaluated, have tested contingency plans, and are certified and accredited.[22]

Since fiscal year 2006, VA's progress in fully implementing the information security program required under FISMA and following the policies issued by OMB has been mixed. For example, from 2006 to 2009, the department reported a dramatic increase in the percentage of systems for which a contingency plan was tested in accordance with OMB policy. However, during the same period, it reported decreases in both the percentage of employees who had received security awareness training and the percentage of employees with significant security responsibilities who had received specialized security training. These decreases in the percentage of individuals who had received information security training could limit the ability of VA to effectively implement security measures.

For fiscal year 2009, in comparison to 23 other major Federal agencies, VA's efforts to implement these information security control activities were equal to or higher in some areas and lower in others. For example, VA reported equal or higher percentages than other Federal agencies in the number of systems for which security controls had been tested and reviewed in the past year, the number of systems for which contingency plans had been tested in accordance with OMB policy, and

---

[20] GAO, *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements,* GAO–10–202 (Washington, D.C.: March 12, 2010).

[21] In March 2007, OMB launched the FDCC initiative to standardize and strengthen information security at Federal agencies. Under the initiative, agencies were to implement a standardized set of configuration settings on workstations with Microsoft Windows XP or Vista operating systems. OMB intended that by implementing the initiative, agencies would establish a baseline level of information security, reduce threats and vulnerabilities, and improve protection of information and related assets.

[22] Certification is a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations based on implementation of controls.

the number of systems that had been certified and accredited. However, VA reported lower percentages of individuals who received security awareness training and lower percentages of individuals with significant security responsibilities who received specialized security training.

Cloud Computing Presents Opportunities but Poses IT Security Challenges

Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers, while freeing them from the burden and costs of maintaining the underlying infrastructure. Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer. The President's budget has identified the adoption of cloud computing in the Federal Government as a way to more efficiently use the billions of dollars spent annually on IT. However, as we reported in May 2010,[23] Federal guidance and processes that specifically address information security for cloud computing had not yet been developed, and those cloud computing programs that have been implemented may not have effective information security controls in place.

As we reported, cloud computing can both increase and decrease the security of information systems in Federal agencies. Potential information security benefits include those related to the use of virtualization, such as faster deployment of patches, and from economies of scale, such as potentially reduced costs for disaster recovery. Risks include dependence on the security practices and assurances of the provider, dependence on the provider, and concerns related to sharing computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation. We made recommendations to OMB, the General Services Administration, and NIST to assist agencies in identifying uses of cloud computing and necessary security measures, selecting and acquiring cloud computing products and services, and implementing appropriate information security controls when using cloud computing.

VA Faces Barriers To Establishing Shared Electronic Health Record Capabilities With DoD

VA and DoD have two of the Nation's largest health care operations, providing health care to 6 million veterans and 9.6 million active duty servicemembers and their beneficiaries at estimated annual costs of about $48 billion and $49 billion, respectively. Although the results of a 2008 study found that more than 97 percent of functional requirements for an inpatient electronic health record system are common to both departments, the departments have spent large sums of money to separately develop and operate electronic health record systems. Furthermore, the departments have each begun multimillion dollar modernizations of their electronic health record systems. Specifically, VA reported spending almost $600 million from 2001 to 2007 on eight projects as part of its Veterans Health Information Systems and Technology Architecture (VistA) modernization. In April 2008, VA estimated an $11 billion total cost to complete the modernization by 2018. For its part, DoD has obligated approximately $2 billion over the 13-year life of its Armed Forces Health Longitudinal Technology Application (AHLTA) and requested $302 million in fiscal year 2011 funds for a new system.

Additionally, VA and DoD are working to establish the Virtual Lifetime Electronic Record (VLER), which is intended to facilitate the sharing of electronic medical, benefits, and administrative information between the departments. VLER is further intended to expand the departments' health information sharing capabilities by enabling access to private-sector health data. The departments are also developing joint IT capabilities for the James A. Lovell Federal Health Care Center (FHCC) in North Chicago, Illinois. The FHCC is to be the first VA/DoD medical facility operated under a single line of authority to manage and deliver medical and dental care for veterans, new Naval recruits, active duty military personnel, retirees, and dependents.

In February 2011, we reported that VA and DoD lacked mechanisms for identifying and implementing efficient and effective IT solutions to jointly address their common health care system needs as a result of barriers in three key IT management areas—strategic planning, enterprise architecture, and investment management.

---

[23] GAO–10–513.

- **Strategic planning:** The departments were unable to articulate explicit plans, goals, and time frames for jointly addressing the health IT requirements common to both departments' electronic health record systems. For example, VA's and DoD's joint strategic plan did not discuss how or when the departments propose to identify and develop joint health IT solutions, and department officials did not determine whether the IT capabilities developed for the FHCC could or would be implemented at other VA and DoD medical facilities.
- **Enterprise architecture:** Although VA and DoD had taken steps toward developing and maintaining artifacts related to a joint health architecture (i.e., a description of business processes and supporting technologies), the architecture was not sufficiently mature to guide the departments' joint health IT modernization efforts. For example, the departments did not define how they intended to transition from their current architecture to a planned future state.
- **Investment management:** VA and DoD did not establish a joint process for selecting IT investments based on criteria that consider cost, benefit, schedule, and risk elements, which would help to ensure that a chosen solution both meets the departments' common health IT needs and provides better value and benefits to the government as a whole.

These barriers resulted in part from VA's and DoD's decision to focus on developing VLER, modernizing their separate electronic health record systems, and developing IT capabilities for FHCC, rather than determining the most efficient and effective approach to jointly addressing their common requirements. Because VA and DoD continued to pursue their existing health information sharing efforts without fully establishing the key IT management capabilities described, they may have missed opportunities to successfully deploy joint solutions to address their common health care business needs.

VA's and DoD's experiences in developing VLER and IT capabilities for FHCC offered important lessons to improve the departments' management of these ongoing efforts. Specifically, the departments can improve the likelihood of successfully meeting their goal to implement VLER nationwide by the end of 2012 by developing an approved plan that is consistent with effective IT project management principles. Also, VA and DoD can improve their continuing effort to develop and implement new IT system capabilities for FHCC by developing a plan that defines the project's scope, estimated cost, and schedule in accordance with established best practices. Unless VA and DoD address these lessons, the departments will jeopardize their ability to deliver expected capabilities to support their joint health IT needs.

We recommended several actions that the Secretaries of Veterans Affairs and Defense could take to overcome barriers that the departments face in modernizing their electronic health record systems to jointly address their common health care business needs, including the following:

- Revise the departments' joint strategic plan to include information discussing their electronic health record system modernization efforts and how those efforts will address the departments' common health care business needs.
- Further develop the departments' joint health architecture to include their planned future state and transition plan from their current state to the next generation of electronic health record capabilities.
- Define and implement a process, including criteria that considers costs, benefits, schedule, and risks, for identifying and selecting joint IT investments to meet the departments' common health care business needs.

We also recommended that the Secretaries of Veterans Affairs and Defense strengthen their ongoing efforts to establish VLER and the joint IT system capabilities for FHCC by developing plans that include scope definition, cost and schedule estimation, and project plan documentation and approval.

Both departments concurred with our recommendations and on March 17, 2011, the Secretaries of Veterans Affairs and Defense committed their respective departments to pursue joint development and acquisition of integrated electronic health record capabilities.

In summary, effective IT management is critical to the performance of VA's mission. However, the department faces challenges in key areas, including systems development, information security, and collaboration with DoD. Until VA fully addresses these and implements key recommendations, the department will likely continue to (1) deliver system capabilities later than expected; (2) expose its computer systems and sensitive information (including personal information of veterans and their beneficiaries) to an unnecessary and increased risk of unauthorized use, disclo-

sure, tampering, theft, and destruction; and (3) not provide efficient and effective joint DoD/VA solutions to meet the needs of our Nation's veterans.

Mr. Chairman, this concludes my statement today. I would be pleased to answer any questions you or other Members of the Subcommittee may have.

Contacts and Acknowledgments

If you have questions concerning this statement, please contact Joel C. Willemssen, Managing Director, Information Technology Team, at (202) 512–6253 or willemssenj@gao.gov; or Valerie C. Melvin, Director, Information Management and Human Capital Issues, at (202) 512–6304 or melvinv@gao.gov. Other individuals who made key contributions include Mark Bird, Assistant Director; Mike Alexander; Nancy Glover; Paul Middleton; and Glenn Spiegel.

MATERIAL SUBMITTED FOR THE RECORD

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 16, 2011

The Honorable Eric K. Shinseki
Secretary
U.S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Mr. Secretary:

In reference to the Oversight and Investigations Subcommittee hearing entitled "Reboot: Examining VA's IT Strategy for the 21st Century" that took place on May 11, 2011, I would appreciate it if you could answer the enclosed hearing questions by the close of business on June 20, 2011.

In an effort to reduce printing costs, the Committee on Veterans' Affairs, in cooperation with the Joint Committee on Printing, is implementing some formatting changes for materials for all full Committee and Subcommittee hearings. Therefore, it would be appreciated if you could provide your answers consecutively and single-spaced. In addition, please restate the question in its entirety before the answer.

Due to the delay in receiving mail, please provide your response to Diane Kirkland at diane.kirkland@mail.house.gov. If you have any questions, please call 202–225–3527.

Sincerely,

Bill Johnson
Chairman

EG/dk

Questions for the Record
House Committee on Veterans Affairs
Subcommittee on Oversight and Investigations
Chairman Bill Johnson
"Reboot: Examining VA's IT Strategy for the 21st Century"
May 11, 2011

Question 1: *Does the VA OI&T have an Enterprise Architecture partner to help realize the benefits of each of the 16 Major Initiatives linked to business outcomes.*

Response: Yes, the Office of Information and Technology (OI&T) Office of Architecture and Strategy uses several partner companies in its work on the Major Initiatives to ensure they are well planned and coordinated. The business sponsor of each major initiative identifies the business goals and objectives they intend to achieve. These outcomes are reviewed and approved by the Deputy Secretary, then monitored on a monthly basis by Office of Policy and Planning (OPP) through Operational Management Reviews. OI&T is building an effective working relationship with the Business Architects in Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA) to create more explicit Enterprise Architecture (EA) artifacts that link in more detail to the Department of Veterans Affairs (VA) Strategic Plan. In turn the Plan links to the Major Initiatives and to OI&T initiatives and the OI&T spend plan. VA is strengthening our approach to using EA to promote mission effectiveness and stewardship of funds.

Question 2: Is Cloud Computing on the multi-year program? What is the desired time frame for its implementation and what are the deciding factors for that time frame?

Response: Cloud computing is not a specific program line item; rather, VA has adopted the direction of the Federal Chief Information Officer (CIO) and has begun implementing a "Cloud First" strategy with any new OI&T initiatives. Agencies are now required to deploy technology projects to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Cloud is increasingly tightly woven into all new VA initiatives.

VA has established criteria for Cloud projects within our enterprise data centers based on storage, processor load and application design.

At this time, we are implementing a private Cloud based in our data centers that provides secure OI&T operations for VA internal systems as well as pursuing commercial Cloud hosting opportunities for VA systems that do not require the same level of security.

The deciding factors in our time frame for deployment include:

- *Security*. Data that contains patient or Veteran financial data obviously requires greater security than, for example, Web sites listing information on obtaining VA services.
- *Applicability for Cloud deployment*. Some applications, because of heavy system requirements, do not lend themselves to virtualization;
- *Application design*. Older applications may be candidates for Cloud, but this requires programming and testing to ensure compatibility;
- *Budget*. Moving to the Cloud involves funding to deploy virtualized systems and storage, as well as for regression testing and standardization of software;
- *Staffing*. VA has a finite number of programmers and operations staff available to provide testing of Cloud services; and
- Availability of secure, reliable, cost-effective commercial services.

There are several VA applications which are in production in a cloud-based architecture or have significant resources invested in their completion. VA currently employs a hybrid private cloud (both off and on premise) to deliver the Post-9/11 GI Bill application suite. The Department continues to work through the technology required to support the movement of 100,000 (approximately 20 percent) customer mailboxes into a Federal cloud architecture, targeted to begin early in fiscal fear 2012. VA has begun beta testing of a private cloud solution for the technology to interface lab equipment with the Department's electronic health care record. These are a few of the varied types of applications which VA has determined were suited for a cloud-based deployment.

Question 3: How has VA's return on investment (ROI) in IT development over the last 5 years compared with private-sector companies of comparable size?

Response: VA's IT ROI compares favorably with the private sector in a number of areas. A recent independent study covering the 10-year period between 1997 and 2007 found that VA's health IT investment was $4 billion, while savings were more than $7 billion. This represents a ROI of 75 percent. In comparison, a 2010 study of General Motors IT investments anticipates an internal ROI of 70 percent.[1] An earlier study of Ford Motor Company's IT investment, on the ford.com Web site, cites a ROI of 115 percent.[2] While the studies' methodologies may differ, the results indicate VA's IT ROI for VistA is similar to comparably-sized private-sector companies.

However, recognizing systemic issues in other areas of development, VA introduced the Project Management Accountability System (PMAS) in 2009 to dramatically increase VA's success rate in meeting customer software milestones. This success rate is now approximately 75 percent, up from 30 percent (estimated, as no metrics were tracked at that time) prior to PMAS implementation.

Question 4: Please describe in further detail how VA's IT investment over the last 5 years has been in line with industry best practices and where improvements can be made.

Response: Prior to the implementation of PMAS in 2009, VA IT investments were not adequately tracked to provide viable answer to this question. Since full implementation of PMAS in March of 2010, VA IT projects have been delivered approximately 75 percent of the customer facing milestones it set. This success rate is in line with industry best practices.

Industry standards for managing IT investments focus largely on the principles and criteria established by the Project Management Institute, widely recognized as the credentialing authority for Project Management Professionals (PMP). These industry standards are constantly evolving. A common thread is the focus on measurable, performance-based oversight techniques that ensure product delivery is com-

---

[1] 2010. General Motors Prepares for Future with Next Generation Information Networks for Global Manufacturing Operations: On Track to Achieve 166 percent ROI Over Five Years. Cisco Business Transformation Series—Connected Manufacturing, page 9. Retrieved from http://www.cisco.com/web/strategy/docs/manufacturing/Cisco-AutoCaseStudy-GM.pdf.

[2] 2002. ROI Profile: Microsoft Content Management Server Ford.com. Nucleus Research Note 17, page 1. Retrieved from http://nucleusresearch.com/library/microsoft-roi/c17.pdf.

pleted within budget, on schedule, and meets performance and functionality expectations.

VA's PMAS is a performance-based project management discipline mandated by VA's Assistant Secretary for Information and Technology for all IT development projects. PMAS conforms to the core principles and standards recognized and utilized by private industry, but PMAS is specifically tailored to manage the unique investment, management, and oversight challenges faced by public sector IT development projects.

PMAS establishes more rigorous controls than the industry standard for ensuring that investments in IT projects meet project development timelines and expectations for functionality. Specifically, PMAS uses incremental product build techniques for IT projects, with delivery of new functionality (tested and accepted by the customer) in cycles of 6 months or less. Projects managed under PMAS are tightly monitored and subject to being halted when significant deviations to plans occur and insufficient remediation plans are presented. PMAS requires that a project be paused and re-evaluated at the point where it has demonstrated trouble.

The use of metrics to monitor and assess performance for IT development is another best practice and key strategy VA employs to ensure resources are used effectively and project managers are held accountable. When PMAS was implemented, we identified a requirement to track, monitor, and report on the status of projects that fell under the PMAS management discipline. As a result, the PMAS Dashboard was developed and fielded. The purpose of the PMAS Dashboard is to track, monitor, and report the status of PMAS managed IT projects—thereby providing visibility into planned versus actual costs and schedules, and to provide a disciplined management approach with the goal to improve the rate of success of VA's IT projects. The status of every active PMAS-managed project is reported to and reviewed by VA senior management on a monthly basis. The implementation of PMAS and related tools has resulted in the on-time delivery of customer-facing products approximately 75 percent of the time, an increase from 30 percent on-time prior to the implementation of PMAS.

PMAS also necessitates the use of VA's standardized development processes. These processes are captured in ProPath, VA's IT process asset library. Process standardization is widely accepted by industry and advisory bodies as a means for improving delivery rate, resource usage, and organizational success. While ProPath initially captured only development practices, later versions of ProPath will capture all aspects of the development lifecycle.

In addition to PMAS, VA adopted a new acquisition strategy to more effectively use our IT resources. This new strategy for acquiring IT services, Transformation Twenty-One Total Technology (T4), will assist to consolidate our IT service requirements into 15 prime contracts (seven of which have been reserved for Veteran-owned small businesses) leveraging economies of scale to save both time and money and enable greater oversight and accountability.

Question 5: Going forward, how will VA OI&T ensure IT contracts are properly defined and written from RFI to RFP to Contract to Implementation—in order to ensure more responsible use of taxpayers' dollars?

Response: VA is using and now strengthening our Integrated Project Team (IPT) process with the right personnel from the beginning of a procurement/acquisition submission to implementation. VA has already published the first IPT guide, and requires as part of PMAS policy, that all projects must be managed under a cognizant IPT. IPT membership is specified in policy, and must include a warranted contracting officer and general counsel. OI&T, OPP, Office of Acquisition, Logistics and Construction (OALC), and Office of General Counsel (OGC) are collaborating in devising several mechanisms to strengthen IPTs. The options under consideration include more training on IPT operation, use of acquisition-trained facilitators for IPT for larger, high-priority programs, and greater management visibility into assignment of staff to IPTs. Customer engagement is required already in policy, but could be strengthened as well to assure timely development of requirements and real-time awareness of project issues that could affect schedule of functionality. This is a teaming relationship with the customer to properly define the requirement so that we are able to design, develop, implement, and deploy the materiel solution needed by the customer. (This is all part of the IPT and PMAS processes, and recorded in ProPATH, the VA OI&T process asset library, which serves as the basis for development of all courseware for OI&T staff training.)

To allow time for IPTs to operate properly and develop practical acquisition strategies, VA is now accelerating the due date for business requirements. For functional requirements for FY 12 projects, the due date will be July 2011.

The following are the practices being utilized at the Technology Acquisitions Center (TAC):

Customer Training—Training provided acquisition-related material to OI&T personnel, covering essential topics such as market research, performance work statements, cost estimates, and technical evaluations. Each of these training units, along with 'hands-on' workshops, were intended to provide the customer with fundamental information that would help them to better understand the acquisition process and associated documentation, thereby resulting in better defined requirements, streamlined processes, and reduced cycle time.

Document Templates—Templates were developed to guide the customer in preparing acquisition plans, sole source justifications, and cost benefit analysis, along with instructional procurement guidelines, which helped customers understand what acquisition documents were required based on the type of procurement and the dollar threshold. One template found most useful was the Performance Work Statement (PWS) template for services, which provided the preparer with detailed guidance through the template. The PWS template has aided in the preparation of requirements which were consistent, accurate, and complete. The introduction of uniformity in the process provides additional assurances that requirements would be more easily understood, and thereby lessen ambiguities which could lead to misinterpretation and undesirable performance.

IPTs and Lockdowns—Two highly effective practices that result in better defined requirements—and ultimately better contracts—is through the use of "IPTs" and "Lockdowns." With roles and responsibilities clearly defined in charters, acquisition and customers work together as integral IPT members in the identification, refinement and establishment of IT requirements and acquisition strategies. While IPTs characterized the components of the partnership, the practice of "lockdowns" provide a real-time, collaborative working framework from which the IPT could excel. With each lockdown session, the objective of critical "buy-in" is achieved as hands-on IPT participants collaboratively formulated business strategies, and established acquisition planning goals, while also jointly developing high-quality technical documentation.

Partnering with Industry—Receiving useful feedback from industry is critical establishing requirements that are both accurate and feasible. Reaching out to industry is a valuable investment of resources, which in the end pays dividends to several beneficiaries. Through "Advanced Planning Briefings for Industry" (APBI) and "Industry Days," cross-communication between industry and the government results in a mutual understanding of the needs and capabilities of the two parties. More specifically, an Industry Day conference allows industry to raise questions and present ideas for Government consideration on a specific, pending requirement. Through these give-and-take forums, the government is provided an opportunity to best define, and refine, its requirements before a solicitation is released.

Question 6: In the Catapult contract, VA OIG found that VA paid Catapult on a milestone basis. This payment basis was inconsistent with both the contract as well as the information provided to vendors during solicitation. What mechanisms are or were in place to prevent blatant disregard of contracting conditions established twice in writing? How did those mechanisms fail twice in the case of this contract?

Response: OI&T is currently conducting an internal review of the Catapult contract. We expect this review to be complete by mid-July, and will plan to brief the Subcommittee when the review is complete.

Question 7: How does an individual or company access GSA's Schedule 70 in order to participate in VA's IT contracting process?

Response: There are over 4,000 companies currently on GSA's Schedule 70. In order to participate in VA's IT contracting process under GSA's Schedule 70, the individual or company must first obtain a GSA Schedule 70 contract. The first step in the process is submitting an offer in response to the IT Schedule 70 solicitation, which is made available on the Federal Business Opportunities (FedBizOpps) Web site. The individual or company would then submit an electronic offer via GSA's eOffer electronic system. GSA would review the offer to ensure compliance with the solicitation, and upon determination that the offeror's prices were fair and reasonable, a GSA IT Schedule 70 contract would be awarded if it was in the best interest of the government. To assist an individual or company, GSA has made available the free online training courses, "How to Become a Contractor—GSA Schedules Program" and "How to Get on Schedule." These courses provide prospective offerors

with helpful information about how to prepare an offer and the GSA Schedule 70 contract award process.

Question 8: In the absence of a final T4 award, is VA moving forward with its IT projects? Is the contracting organization denying the program managers alternative contracting vehicles in anticipation of using T4?

Response: VA is, and will continue to move forward on all of its IT projects. The VA's contracting organizations will continue to take into consideration all available contractual vehicles in the development of an acquisition strategy. This procedure will continue irrespective of the T4 awards.

Question 9: What assurance can VA provide the Committee that VA will use other contracting vehicles that are currently available in order to move IT projects forward?

Response: Since January 1, 2011, OI&T has awarded 218 contracts (through June 1, 2011) using various contracting vehicles. We will continue to perform work while we await T4 award.

Question 10: What steps has VA taken to ensure success for the Interagency Program Office (IPO) as "the single point of accountability" as established in the FY 2008 National Defense Authorization Act? How has VA defined "single point of accountability" in writing to those involved with the IPO?

Response: VA will be utilizing the IPO as established by the FY 2008 National Defense Authorization Act. VA and DoD are currently revising IPO's charter to empower the IPO to effectively manage the implementation of the integrated Electronic Health Record (iEHR).

Question 11: Please describe in further detail the cooperative actions, below the Secretary level, between VA and DoD in implementing iEHR.

Response: The Secretaries have designated the Deputy Chief Management Officer (DoD) and the Assistant Secretary, Information and Technology (VA) to lead the coordinated efforts of the two Departments to establish the iEHR through a Senior Coordinating Group (SCG). The Secretaries have charged the SCG with accomplishing the initial objectives of the iEHR, including establishing governance, naming key staff, and planning the implementation of the iEHR, including costing. There are hundreds of VA and DoD staff working on accomplishing the various taskings as assigned by the SCG.

Question 12: Please describe in further detail DoD's role in the move toward Open Source and how that role has compared to VA's actions.

Response: Clearly, establishing an Open Source consortium, and embracing private-sector participation in VistA, was initially driven by VA. After considering the role that Open Source could play in ensuring the long-term success of the iEHR, particularly in helping the government better engage the private sector, DoD agrees with VA that Open Source is a vital part of the path forward for the iEHR. To that end, DoD is participating in both the selection of the Custodial Agent (CA) and in the Board of Directors of the CA.

Question 13: The National Institute of Standards and Technology (NIST), in its Internal Report 7622 (NISTIR 7622) published last year, sets of supply chain risk management practices for Federal information systems. Has VA applied these practices to its own IT projects? What steps has VA taken to minimize supply chain risk for IT projects?

Response: VA OI&T minimizes supply chain risk management by managing the security component of all software development and service delivery work. OI&T does not outsource the security component when purchasing products and services. OI&T has developed tight security controls in line with the NIST recommendations, as well as FISMA requirements, which allows us to provide the necessary standards to manage supply chain risk.

Question 14: Has the IPO been utilized in any of these steps? If so, which ones?

Response: As VA and DoD move forward with plans to strengthen the IPO's charter, supply chain risk management best practices will be one of the many factors considered.

Question 15: Please further explain VA's certainty in the Open Source approach when, by VA's own admission, no cost analysis had been done ahead of time. Other than a three-page document provided to the Subcommittee after the May 11 hear-

ing, what documentation explains in detail the review of all alternatives before making a decision?

Response: The cost analysis for Open Source is short because the analysis is simple. VA has proven that the EHR is a vital part of effective heath care for Veterans. Our current EHR, VistA, while still viable is no longer the market leader VA assesses the cost of replacing VistA at its 153 hospitals and over 800 CBOCs at approximately $16 billion. If VA cannot find a way to move VistA forward at a rate that keeps pace with the private sector, we must eventually ask the taxpayers for the funding necessary to replace VistA. Our assessment is that Open Source is a viable path, and perhaps the only viable path, to allow VA to improve VistA at a much more rapid pace by involving the private sector in both planning and implementing its path forward. As DoD and VA move forward to establish the iEHR, the involvement of the private sector is even more critical, which is one of the primary reasons DoD has agreed with VA that Open Source should be part of our overall iEHR plans.

VA has spent more than a year conducting a very deliberative process to examine the implications of Open Source for VistA. We have seen two substantial studies on the topic contributed by the private sector and academia. We have consulted with hundreds of organizations, and thousands of individuals about the pros and cons of the Open Source approach. We have conducted three Requests for Information (RFIs), and received numerous papers, emails, and comments. Our path forward with Open Source has been broadly advised and is highly transparent.

Question 16: Please identify and explain the elements of VA's life-cycle analysis of IT projects.

Response: IT projects are selected based on their relationship to the VA Strategic Plan. The single IT authority at VA allows comprehensive view of all VA IT investments and their prioritization using a shared governance approach in concert with their respective business sponsors. To create a lifecycle view of total cost of ownership, VA is in the process of implementing IPTs for all projects, which includes members with the knowledge of life cycle management, to address all infrastructure components from data center to desktop, from project initiation to close out and disposal.

Question 17: Please explain how VA applied the above life-cycle analysis to Open-Source VistA prior to making the decision to move forward on that project.

Response: VA senior leadership has determined that as a software sourcing strategy, Open Source (OS) represents an approach that is very likely to reduce development risk and strengthen development rigor, promote innovation, promote cyber security, and make OS applications more broadly available to the Nation through the entire life cycle of each OS project. Open Source is a development strategy, and is not itself a project with a life cycle—and, it is not a substitute for life cycle management of total cost of ownership. The OS approach will allow VA to address total cost of ownership for Open Source software, including implementation, hosting, telecommunications, end-user support, and project closeout.

Question 18: Is VA appropriately staffed with the knowledge and experience level to build rigorous business cases based on comprehensive cost benefit analyses and returns on investment in information technology?

Response: While no organization is at a point where it has all of the expertise and knowledge it needs, VA OI&T has made great strides towards building an IT staff with the knowledge and skills required to accomplish our mission. Through our Program/Project Manager training courses, peer review process, techstat meetings, competency model, and other training and guidance practices, OI&T has worked to develop tools to improve the performance of our staff.

Question 19: Please describe OI&T's incorporation of Supply Chain Risk Management by the National Institute of Standards and Technology (NIST) in moving forward with Open Source software implementation.

Response: As discussed above, OI&T's Information Security organization effectively and directly manages the security component of software development, procurement, and implementation. We will continue to employ these best practices in moving forward with the Open Source software implementation.

Question 20: DoD is currently running pilot programs on cybersecurity. Please explain VA's decision to move forward on large-scale IT programs before these programs have concluded and the results have been published.

Response: VA has determined that delay in pursuing its operational requirements for critical programs such as Veterans Benefits Management System (VBMS), Post-9/11 GI Bill, and VistA Open Source, should not be delayed due to DoD's pilot programs. This assessment considered the pressing needs to improve performance and service delivery to Veterans as well as the status of each program. VA will ensure its cybersecurity requirements are fully integrated into all projects and will maintain close contact with DoD in order to consider the emerging outcomes of their pilot programs.

Question 21: According to a number of industry white papers, Wi-Fi has deficiencies as a real-Time Asset and Patient Tracking Solution and ultimately will cost more to use this method than radio frequency identification technology (RFID) for the same purpose. On June 17, 2010, VA (10N) placed a moratorium on Real Time Location systems acquisition because a national contract was to be implemented during that fiscal year. Is the moratorium still in place? If so, please explain VA's recent submissions of two RFP's with language that indicates Infra-red and Radio Frequency work-arounds while the moratorium is in place?

Response: Real-Time Location Systems (RTLS) and radio frequency identification (RFID) are closely related, and are overlapping technologies used for identifying and locating items or people. RTLS is the term used to describe those technologies that provide "real-time" location, regardless of whether radio frequencies are used or some other technology, such as ultrasound or infra-red. RFID is the term used to indicate that radio frequencies are being utilized, regardless of whether the item is being located in real-time or not. Therefore, some RTLS systems are also RFID systems, and some RFID systems are also RTLS systems. They are not necessarily separate systems that compete with one another. Rather, the terms offer differing ways of describing these systems, either by describing the technologies employed or the uses for the technologies. RFID is generally broken down into two types: passive and active. Active RFID systems utilize a tag with a battery, that beacons information at pre-set intervals. Passive RFID systems utilize a "tag" (normally a sticker or label) that has no battery, so relies on an external power source to "excite" it, causing it to send out an identification message. Because passive RFID tags only announce themselves when in the proximity of an exciter, passive systems generally do not offer real-time location capabilities.

VA has a large number of business processes (use cases) that can benefit from RTLS and/or RFID technologies. Some use cases lend themselves to passive RFID, while others lend themselves to active RFID/RTLS. An example of the former is folder accountability and inventorying in VBA, while an example of the latter is real-time location of mobile medical assets, such as EKG carts, infusion pumps, or wheelchairs. Because VA has such a wide variety of use cases, it was understood from the beginning that no single RFID/RTLS technology would satisfy all of VA's needs. It is therefore VA's plan to procure an appropriate technology to address each use case.

Even within active RFID, there are numerous technologies, each with their own unique set of plusses and minuses. Wi-Fi is a radio frequency (RF) based system utilizing the 2.4 GHz band. There are also RF based systems utilizing the 900 MHz and 433 MHz bands. Additionally, there are systems that utilize ultrasound (either alone or in combination with an RF-based system) or an infra-red system in combination with an RF-based system.

Prior to making the decision to utilize Wi-Fi for RTLS, when possible, VA consulted with industry leaders such as Gartner. Gartner indicated that Wi-Fi has the single largest market share, by far, in the health care RTLS market space, (likely exceeding 60 percent) and that when a properly configured WiFi network is already in place, it makes sense to leverage the existing investment for location-based services such as RTLS, rather than wiring and installing redundant networks of transceivers, at great cost, for little or no benefit. Cost, however, is not the only consideration. One of VA's major concerns is interoperability and not being locked into a proprietary, single-vendor solution. WiFi-based RTLS systems are the only standards-based RTLS solution, being based on the international IEEE 802.11 standard. Other systems (notably, those based on 900 MHz, 433 MHz, and ultrasound) are highly proprietary, meaning that one vendor's tags will not work with any other vendor's transceivers, even if the same frequency band is utilized. This creates two potentially dangerous conditions for VA: the possibility of the single vendor going out of business, and the possibility of the single vendor raising the cost of the proprietary tags by an exorbitant amount. VA finds it more prudent to employ technologies based on internationally-recognized standards, where consumables (in this case, RTLS tags) are commodities, available from multiple vendors.

Wi-Fi based RTLS systems currently have a spatial resolution of approximately 7 meters at best, although as technology advances, this is improving. For some purposes, it is sufficient to know where an item is to within 7 meters accuracy. It is for those use cases only that VA intends to utilize Wi-Fi alone. It is well understood that some use cases in VA require pinpointing an item's location with greater accuracy than 7 meters, and it is our intention to procure complementary technologies (infra-red or ultrasound) in those cases. This is not a work-around for a flawed system. Use of hybrid systems is a common strategy employed by RTLS vendors and customers to leverage the benefits of Wi-Fi, yet augment it (where necessary) to provide finer spatial resolution than could be achieved by Wi-Fi alone. It should be noted that other RF-based systems (e.g. 433 and 900 MHz) also require these same complementary technologies to enhance spatial resolution for certain use cases.

Given the promise that RFID and RTLS systems have for VA operations, multiple VA entities have identified the need for these systems and had begun to procure them. Unfortunately, this was being done in an uncoordinated fashion, with no technical standards and no thought to interoperability. If these systems are to be maximally useful, they must be able to exchange data and be able to aggregate data at a national level. Commonality is also required in order to support higher quality, more efficiency, and less costly. This was the impetus behind the moratorium. It was designed to afford VA the opportunity to devise a technical strategy for RFID/RTLS so that taxpayer dollars would be used wisely.

The RTLS/RFID moratorium is still in place, while VA crafts a national RFP and awards an intended indefinite delivery/indefinite quantity (IDIQ) contract to satisfy all RTLS/RFID needs. Although significant market research has been done, and is continuing, the extremely large scope of the RTLS initiative made it prudent to perform several technology demonstrations. The two RFPs cited are part of VA's carefully controlled technology demonstrations. Veterans Integrated Service Networks (VISNs) 10 and 11 have been given permission to procure RTLS/RFID systems, in very specific configurations, prior to award of the national IDIQ contract. It is hoped that the lessons learned from these technology demonstrations will aid us in the implementation and use of RTLS/RFIS systems nationally, and help shape future technology choices.

Question 22: The National Project Management Office (PMO) for Real Time Location Systems (RTLS) is touted as the Center of Excellence for those systems, yet, contrary to industry standard, it is pursuing 802.11 technology for location services despite known limitations of 802.11 for that purpose. Please explain in detail the reason for using 802.11 and the reasons for not using Infra-red and Radio Frequency methodologies, two technologies generally regarded as better suited for location services and other uses.

Response: VA performed extensive market research on the various technologies, including consulting with the firm generally considered to be the leader in information technology (IT) consulting, Gartner. It is VA's understanding that Wi-Fi based RTLS systems command the lion's share of the market for health care RTLS—over 50 percent. That would make it very much the "industry standard." Additionally, it is not VA's intention to use Wi-Fi systems alone, except where it meets the business need. Whenever a greater spatial resolution is needed than Wi-Fi alone can provide, VA intends to use Wi-Fi along with a complementary technology, such as infra-red or ultrasound. Part of VA's motivation for performing the technology demonstrations in VISNs 10 and 11 is to generate first-hand knowledge of the benefits and disadvantages of each of the major RTLS technologies in a VA environment, so that we need not rely on information from external sources that may or may not be relevant to VA.

VA is not aware of any compelling data to suggest that a hybrid system utilizing Wi-Fi and a complementary technology (when necessary) is inferior to other RTLS technologies on the market.

Question 23: How does VA OI&T address Wi-Fi's incompatibility with existing structures that result in a need for more access points to triangulate tags and higher long-run costs compared to other technologies?

Response: The need for additional access points is primarily related to the desire to support voice over Wi-Fi (VoWiFi). The number of additional Wi-Fi- access points needed to support RTLS (as compared to VoWiFi) is small—estimated to be an additional 10 percent or less. It is hard to understand how a non-WiFi RTLS system could demonstrate lower long-term costs than a WiFi-based RTLS system, when an organization already has a WiFi infrastructure in place capable of providing location-based services. Implementing a non-WiFi RTLS system would require pulling cable for hundreds of additional transceivers per facility, purchasing and installing

those transceivers, potentially running electrical connections for those transceivers, and then providing ongoing support and maintenance for the non-WiFi RTLS transceivers (in addition to the WiFi access points that would still be needed for other business purposes). WiFi-based tags can be moderately more costly than non-WiFi tags, (perhaps $50 per tag instead of $40) but the number of RTLS tags per facility would need to be huge in order to make up the excess cost (up front and ongoing) associated with the non-WiFi infrastructure. It should also be noted that with a WiFi-based RTLS system, any device that already has WiFi built in does not need a tag, since its existing WiFi radio acts as an RTLS tag. In addition to devices like laptops, tablets, and smart phones, more and more medical devices now come equipped with WiFi radios, further saving on RTLS tag costs.

Question 24: Are additional technologies necessary to achieve better accuracy in location and tracking services, at a minimum, and if so, are additional infrastructures needed?

Response: As discussed more fully in question 21, WiFi suffices for some of VA's many RTLS use cases, while for others, it does not. Where a use case demands greater spatial resolution than WiFi alone can provide, VA intends to utilize complementary technologies, such as ultrasound or infra-red, on an as-needed basis.

Question 25: Does VA utilize RFID/RTLS technology that provides multiple uses on the same infrastructure?

Response: VA currently has only very limited deployment of RTLS. However, the plan, as currently envisioned, allows us to leverage the same infrastructure (WiFi) for multiple business purposes, including wireless data (Bar Code Medication Administration [BCMA], bedside nursing admissions, bedside progress notes, etc) and voice (wireless WiFi-based phones).

Question 26: How do these Wi-Fi solutions track objects outside the building using the same infrastructure versus other technologies that have both indoor and outdoor solutions built-in?

Response: None of the initial use cases for VHA involve tracking items outdoors. WiFi can be utilized for outdoor use cases, when the item will remain on campus. If inter-facility location-finding is needed, some other technology, such as GPS, would likely be utilized.

Question 27: How does VA OI&T deal with the latency in Wi-Fi between when a message is sent and received, potentially triggering alarms and, for example, locking a door before a patient is able to exit?

Response: There is no industry consensus on whether WiFi is slower or has greater latency than competing systems, but OI&T does not believe this to be an issue. However, if latency issues were a concern, quality of service controls could be instituted to ensure that RTLS traffic would get priority.

Question 28: Do VA's Wi-Fi solutions send encrypted data vulnerable to a security breach?

Response: The VA Wi-Fi utilizes equipment that is FIPS 140–2 Certified (mandated by FISMA and VA Handbook 6500) and is configured to follow the associated FIPS 140–2 Security Policy as well as following NIST Special Publication 800–97: Establishing Wireless Robust Security Networks. The system is based on 802.11i WPA2/AES security protocols which utilize FIPS 140–2 certified cryptographic modules.

Question 29: How do these solutions keep running if there is an issue with the Wi-Fi infrastructure or access points at any given time?

Response: The Wi-Fi Infrastructure is setup and configured to survive single component failure at the controller in the N+1 design model. The access points (AP) are deployed and configured in a way in which the system self heals. That is, the infrastructure will see an AP "drop off" and will increase signal strength in surrounding APs to cover the deficiency automatically.

Question 30: How will the cost of batteries in Wi-Fi tags affect long-term usage and cost versus other low-power consumption technologies?

Response: Our market research indicates that battery life with WiFi-based tags will be comparable to that seen in other active RTLS tags. By adjusting the beacon rate, a battery life of 2 years or more should be attainable. Necessary beacon rate will vary by use case.

Question 31: How will interface from Wi-Fi in everyday devices carried by people in facilities affect the tracking of tags in any VA facility?

Response: Although this has been raised as a concern, at least 60 percent of the health care RTLS market utilizes WiFi-based systems, and interference from other WiFi devices has not been shown to be a significant problem.

Question 32: VA OI&T currently has a workforce of over 7,100 people. Please outline the growth of that staff over the last 2 years as well as anticipated future growth.

Response: At the beginning of FY 2009, OI&T staff count was 6,645. The current (as of April) staff count is 7,101. OI&T's planned end-of-FY 2011 staff count is 7,271. We are not requesting a staffing increase as part of our FY 2012 budget.

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 12, 2011

The Honorable Roger W. Baker
Assistant Secretary for Information
Technology and Chief Information Officer
U.S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Secretary Baker:

I would like to request your response to the enclosed questions for the record and deliverable I am submitting in reference to our House Committee on Veterans' Affairs Subcommittee on Oversight and Investigations hearing on *Reboot: Examining VA's IT Strategy for the 21st Century* on May 11, 2011. Please answer the enclosed hearing questions and deliverables by no later than Wednesday, June 22, 2011.

In an effort to reduce printing costs, the Committee on Veterans' Affairs, in cooperation with the Joint Committee on Printing, is implementing some formatting changes for material for all full Committee and Subcommittee hearings. Therefore, it would be appreciated if you could provide your answers consecutively on letter size paper, single-spaced. In addition, please restate the question in its entirety before the answer.

Due to the delay in receiving mail, please provide your response to Ms. Orfa Torres by fax at (202) 225–2034. If you have any questions, please call (202) 225–9756.

Sincerely,

Joe Donnelly
Ranking Member

MH/ot

Questions for the Record
House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Ranking Member Joe Donnelly
"Reboot: Examining VA's IT Strategy for the 21st Century"
May 11, 2011

Question 1: What are we doing to convert the many contracted IT staff positions to Full Time Employee (FTE) positions within the VA?

Response: The Office of Information and Technology (OI&T) is already positioning itself to recruit, retain, and train staff to have needed specialized skills through the use of our staff competency models, which are currently under development. These models will also be deployed to help ensure that VA has the continuously strong, capable leadership corps that it needs, and that leaders have the skills and proficiency to lead people and progress. However, in instances where specialized knowledge is needed for short duration, OI&T will continue to use contracted services, which provides a more cost-effective alternative to hiring full-time career Federal employees.

Question 2: According to the VA OIG's recent report on the contract awarded to Catapult, their findings concluded that information provided to the vendor was unreliable. The documents proved to be incomplete or reliable, and the VA was aware of this. Why did VA continue with the procurement process knowing documents were incomplete or unreliable?

Response: OI&T is currently conducting an internal review of the Catapult contract. We expect this review to be complete by mid-July, and would appreciate the opportunity to provide a brief on our findings when the review is complete.

Question 3: The VA OIG was unable to determine if Catapult was in compliance with the Federal Acquisitions Regulation (FAR), because the VA did not request documentation on the subcontractors to ensure compliance with the FAR provision. Why would the VA not request or have this documentation available?

Response: VA wants to clarify that we believe this question refers to the Office of Inspector General (OIG) Report discussion of possible non-compliance with FAR 52.219–27, which requires that specific minimum percentages of the labor cost be paid to the employees of the vendor or of another Service-Disabled Veteran-Owned Small Business (SDVOSB)*. The OIG Report refers only to the 50 percent minimum level; the installation of WiFi networks may well fall into the category of "Construction by special trades contractors" which specifies a 25 percent minimum level. We are aware that Catapult has stated in writing that they are in compliance with the FAR; we are not aware of what specific data they may have provided to the OIG to verify compliance.

*The following minimum percentages are specified by FAR 52.219–27:

1. Services (except construction), at least 50 percent of the cost of personnel for contract performance will be spent for employees of the concern or employees of other service-disabled Veteran-owned small business concerns;
2. Supplies (other than acquisition from a nonmanufacturer of the supplies), at least 50 percent of the cost of manufacturing, excluding the cost of materials, will be performed by the concern or other service-disabled Veteran-owned small business concerns;
3. General construction, at least 15 percent of the cost of the contract performance incurred for personnel will be spent on the concern's employees or the employees of other service-disabled Veteran-owned small business concerns; or
4. Construction by special trade contractors, at least 25 percent of the cost of the contract performance incurred for personnel will be spent on the concern's employees or the employees of other service-disabled Veteran-owned small business concerns.

As stated above,OI&T is currently conducting an internal review of the Catapult contract. We expect this review to be complete by mid-July, and would appreciate the opportunity to provide a brief on our findings when the review is complete.

Question 4: In your response to the Committee on the letter we sent on March 25th inquiring about Open Source, you said that DoD's participation in Open Source VistA is not essential. Can you elaborate on this?

Response: This question is now moot, as DoD has joined VA in support of the Open Source approach. Had DoD not joined in the Open Source approach, VA would have used to the Open Source approach to develop and accomplish the changes necessary to VistA to move it towards compliance with the integrated EHR (iEHR) architecture as defined by VA and DoD. While this is still the plan, both DoD and VA expect that the Open Source will be a viable way of identifying, selecting, and implementing modules of the iEHR that we jointly identify.

Question 5: What is being done to balance the needs of IT security, while still having a common sense approach to meet needs of employees and veterans? (example: still do not have wireless Internet in VA facilities because of security fears, even though the public hospitals all have them)

Response: Because of past events, VA clearly holds itself to a higher standard than previous years for information security and information protection. OI&T is working hard to strike a balance between our information security needs and convenient network use, while providing the tools and access needed by employees and Veterans. OI&T's information security team has developed strong information security controls on the wireless networks currently online in the hospitals with this capability. For medical centers without wireless access, the current concern is resolv-

ing conflicts with wireless medical devices, as well as the physical impediments to wireless access in large medical centers.

OI&T and VHA are currently piloting a program by a third party vendor to provide wireless Internet access in the lobby and waiting areas of medical centers for Veterans to use.

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 12, 2011

Ms. Belinda J. Finn
Assistant Inspector General for Audits and Evaluations
Office of Inspector General
U.S. Department of Veterans Affairs
801 I Street, NW
Washington, DC 20001

Dear Ms. Finn:

I would like to request your response to the enclosed questions for the record I am submitting in reference to our House Committee on Veterans' Affairs Subcommittee on Oversight and Investigations hearing on *Reboot: Examining VA's IT Strategy for the 21st Century* on May 11, 2011. Please answer the enclosed hearing questions and deliverables by no later than Wednesday, June 22, 2011.

In an effort to reduce printing costs, the Committee on Veterans' Affairs, in cooperation with the Joint Committee on Printing, is implementing some formatting changes for material for all full Committee and Subcommittee hearings. Therefore, it would be appreciated if you could provide your answers consecutively on letter size paper, single-spaced. In addition, please restate the question in its entirety before the answer.

Due to the delay in receiving mail, please provide your response to Ms. Orfa Torres by fax at (202) 225–2034. If you have any questions, please call (202) 225–9756.

Sincerely,

Joe Donnelly
Ranking Member

MH/ot

U.S. Department of Veterans Affairs
Washington, DC.
June 13, 2011

The Honorable Joe Donnelly
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
United States House of Representatives
Washington, DC 20515

Dear Congressman Donnelly:

This is in response to your May 12, 2011, letter following the May 11, 2011, hearing on *Reboot: Examining VA's IT Strategy for the 21st Century.* Enclosed are our responses to the additional hearing questions.

Thank you for your interest in the Department of Veterans Affairs.

Sincerely,

GEORGE J. OPFER
Inspector General

Enclosure

Questions for the Record from the
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
United States House of Representatives
Hearing on
Reboot: Examining VA's IT Strategy for the 21st Century

Question 1: From a VA OIG perspective, what steps has VA taken to improve its ability to manage information technology (IT) projects?

Response: VA's Office of Information and Technology (OI&T) recognized that it has issues with its program management abilities to ensure that IT development efforts are successful. To manage this shortfall, OI&T established the Project Management Accountability System (PMAS), a performance based management discipline that requires frequent delivery (at least every 6 months) of IT functionality. PMAS is currently schedule-driven, allowing for flexibility in project scope and functionality to ensure the schedule can be met. Under PMAS, three consecutive failures ("3 strikes") to meet a scheduled project deliverable will result in a project being "paused." At the "paused" stage, the project is assessed to determine if it should be continued or terminated. PMAS also includes a red flag process which allows anyone associated with a project to elevate project-related issues to senior level officials so that they can take corrective actions quickly.

Further, OI&T is emphasizing Agile versus a traditional software development methodology, in which a project moves sequentially through concept, design, testing, and implementation phases. Agile is an iterative and incremental software development methodology that allows for requirements and solutions to evolve through team collaboration and interaction. Agile is intended to accomplish the following:

- Emphasize teamwork.
- Promote a disciplined project management process that encourages frequent inspection and adaptation by breaking tasks into small increments with minimal planning.
- Complement PMAS' requirement for frequent delivery of deployable IT system functionality.

Question 2: Can you explain the purpose of your current PMAS audit?

Response: We are assessing whether OI&T has taken appropriate steps in implementing PMAS. Our audit will determine whether:

- An adequate plan was in place for PMAS implementation.
- Resources are available and assigned to carry out PMAS.
- PMAS staff roles and responsibilities have been defined.
- PMAS Dashboard data for monitoring project status and progress are reliable.
- Controls such as oversight reviews, cost tracking mechanisms, and step-by-step guidance are in place to ensure projects are not only meeting schedule, but also cost and performance goals.

These areas reflect issues we have historically identified in other audits of OI&T system development initiatives.

Question 3: Do you see problems with PMAS' incremental delivery and managing development projects to schedule?

Yes. Stakeholders have expressed concerns about disrupted operations when they do not receive planned functionality on time and the time it may take to produce all the required functionality under the incremental delivery approach. Further, the potential exists that once functionality is fully delivered it may be obsolete.

For example, we reported, in our audit of the Post-9/11 GI Bill Long Term Solution (LTS), that managing a project primarily to schedule may be at the risk of performance and cost (*Audit of VA's Implementation of the Post-9/11 GI Bill Long Term Solution,* September 30, 2010). During certain phases of LTS development, the project met schedule, but did not provide the originally intended functionality. The project did not receive a strike even though the functionality delivered was significantly less than planned.

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 12, 2011

Mr. Joel Willemssen
Managing Director, Information Technology
U.S. Government Accountability Office
Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Willemssen:

I would like to request your response to the enclosed question for the record I am submitting in reference to our House Committee on Veterans' Affairs Subcommittee on Oversight and Investigations hearing on *Reboot: Examining VA's IT Strategy for the 21st Century* on May 11, 2011. Please answer the enclosed hearing questions and deliverables by no later than Wednesday, June 22, 2011.

In an effort to reduce printing costs, the Committee on Veterans' Affairs, in cooperation with the Joint Committee on Printing, is implementing some formatting changes for material for all full Committee and Subcommittee hearings. Therefore, it would be appreciated if you could provide your answers consecutively on letter size paper, single-spaced. In addition, please restate the question in its entirety before the answer.

Due to the delay in receiving mail, please provide your response to Ms. Orfa Torres by fax at (202) 225–2034. If you have any questions, please call (202) 225–9756.

Sincerely,

Joe Donnelly
Ranking Member

MH/ot

U.S. Government Accountability Office
Washington, DC.
June 22, 2011

The Honorable Joe Donnelly
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
House of Representatives

Subject: *Reboot: Examining the Department of Veterans Affairs Information Technology Strategy for the 21st Century*

This letter responds to your recent question related to our May 11, 2011, testimony on the Department of Veterans Affairs' (VA) ongoing information technology (IT) management challenges.[1] At that hearing, we discussed VA's weaknesses in managing its IT resources, particularly in the areas of systems development, information security, and collaboration with the Department of Defense (DoD) on efforts to meet common health system needs. Your question, along with our response, follows.

In your opinion, what specific actions does the VA IT office need to focus on to capitalize on current technologies available?

VA can take a number of specific actions to capitalize on available IT. As discussed in our prior reports and summarized in our recent testimony,[2] the following actions could help VA address challenges in improving system development, strengthening information security, and increasing collaboration with DoD.

Improve system development: VA has historically experienced significant IT system development difficulties and can improve two projects that have yielded mixed results. For its outpatient appointment scheduling project, which spent an estimated $127 million over 9 years without implementing any of the planned capabilities, the department can improve its acquisition plans, identify complete system

[1] GAO, *Information Technology: Department of Veterans Affairs Faces Ongoing Management Challenges,* GAO–11–663T (Washington, D.C.: May 11, 2011).
[2] GAO–11–663T.

requirements, adhere to system testing guidance, increase earned value management data reliability, manage project risks, and provide effective oversight.[3] Additionally, although VA has partially delivered new system capabilities to process education benefits provided under the Post-9/11 GI Bill, the department can improve its effort to complete the system. In particular, to guide the full development and implementation of the new system, VA can create project performance measures, establish traceability between system requirements and legislation, define criteria for what constitutes the system being "done," improve system testing, and implement a project oversight tool.

Strengthen information security: Effective information security is essential to securing the systems and information on which VA depends to carry out its mission. Without proper safeguards, the department's systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. In recent years, VA has reported an increasing number of security incidents and events. The department can improve its security posture by implementing the recommendations of its Office of Inspector General for strengthening access controls, configuration management, change management, and service continuity. Also, the department can fully implement the requirements of the Federal Desktop Core Configuration (FDCC) initiative, including implementing a baseline set of configuration settings, acquiring and deploying an FDCC compliance tool, and implementing a policy to monitor compliance.[4] Additionally, VA should ensure that any use of cloud computing that the department undertakes includes implementation of appropriate information security controls.

Increase collaboration with DoD: VA and DoD have two of the Nation's largest health care operations, providing health care to 6 million veterans and 9.6 million active duty servicemembers and their beneficiaries at estimated annual costs of about $48 billion and $49 billion, respectively. Although the results of a 2008 study found that more than 97 percent of functional requirements for an inpatient electronic health record system are common to both departments, VA and DoD face barriers to identifying and implementing efficient and effective IT solutions to jointly address their common health care system needs. Thus, we have recommended several actions that VA can take, in conjunction with DoD, to overcome the barriers they face as they modernize their electronic health record systems. We specifically recommended that the departments improve their strategic planning, further develop their joint health architecture, and define and implement a process for identifying and selecting joint IT investments.[5]

In summary, these actions are intended to address the challenges VA faces in improving system development, strengthening information security, and increasing collaboration with DoD and could help the department better capitalize on IT.

To respond to this question, we relied on previously reported information, as well as information collected through follow-up with the department. The work supporting these reports was conducted in accordance with generally accepted government auditing standards. These 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.

Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512–6253 or willemssenj@gao.gov.

Sincerely yours,

Joel C. Willemssen
Managing Director, Information Technology

[3] 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).

[4] GAO, *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements,* GAO–10–202 (Washington, D.C.: March 12, 2010).

[5] GAO, *Electronic Health Records: DoD and VA Should Remove Barriers and Improve Efforts to Meet Their Common System Needs,* GAO–11–265 (Washington, D.C.: February 2, 2011).