THE U.S. DEPARTMENT OF VETERANS AFFAIRS INFORMATION TECHNOLOGY REORGANIZATION: HOW FAR HAS VA COME?

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

SEPTEMBER 26, 2007

Serial No. 110–47

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE

39–456 WASHINGTON : 2008

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

BOB FILNER, California, *Chairman*

CORRINE BROWN, Florida
VIC SNYDER, Arkansas
MICHAEL H. MICHAUD, Maine
STEPHANIE HERSETH SANDLIN, South Dakota
HARRY E. MITCHELL, Arizona
JOHN J. HALL, New York
PHIL HARE, Illinois
MICHAEL F. DOYLE, Pennsylvania
SHELLEY BERKLEY, Nevada
JOHN T. SALAZAR, Colorado
CIRO D. RODRIGUEZ, Texas
JOE DONNELLY, Indiana
JERRY MCNERNEY, California
ZACHARY T. SPACE, Ohio
TIMOTHY J. WALZ, Minnesota

STEVE BUYER, Indiana, *Ranking*
CLIFF STEARNS, Florida
JERRY MORAN, Kansas
RICHARD H. BAKER, Louisiana
HENRY E. BROWN, JR., South Carolina
JEFF MILLER, Florida
JOHN BOOZMAN, Arkansas
GINNY BROWN-WAITE, Florida
MICHAEL R. TURNER, Ohio
BRIAN P. BILBRAY, California
DOUG LAMBORN, Colorado
GUS M. BILIRAKIS, Florida
VERN BUCHANAN, Florida

Malcom A. Shorter, *Staff Director*

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

September 26, 2007

THE U.S. DEPARTMENT OF VETERANS AFFAIRS INFORMATION TECHNOLOGY REORGANIZATION: HOW FAR HAS VA COME?

WEDNESDAY, SEPTEMBER 26, 2007

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

The Committee met, pursuant to notice, at 9:58 a.m., in Room 334, Cannon House Office Building, Hon. Bob Filner [Chairman of the Committee] presiding.

Present: Representatives Filner, Snyder, Herseth-Sandlin, Hare, Salazar, Walz, Buyer, Stearns, Brown of South Carolina, Brown-Waite, Bilbray, and Lamborn.

OPENING STATEMENT OF CHAIRMAN FILNER

The CHAIRMAN. This meeting of the House Committee on Veterans' Affairs is called to order. Today, the Committee will be looking at the U.S. Department of Veterans Affairs (VA) Information Technology (IT) Reorganization: How Far Have We Come?

Obviously, this is a very important issue. And we will be looking at the progress of VA in centralizing its IT efforts.

We want to explore the progress that the VA has made in its efforts to be what Secretary Nicholson called the "gold standard" of information security among Federal agencies, a goal that was enunciated in the wake of a data breach last year that involved over 25 million veterans and succeeding incidents including one recently in Birmingham, Alabama.

We understand that such a centralization will not happen overnight. We are not asking you to do this overnight. But we are asking, and our veterans are demanding, that the VA be held accountable for getting the job done.

This past June, the U.S. Government Accountability Office (GAO), while praising the commitment from senior leadership, found fault with a number of areas in the VA's efforts, efforts that hinder the VA's ability to successfully reach its reorganization goals.

These include rejecting the GAO's recommendation that VA create a dedicated implementation team responsible for day-to-day management of major change initiatives. Instead, the VA is apparently dividing the responsibility among two organizations in this new structure. And the GAO was concerned that this approach would not work. Many of us on this Committee share that sense.

More recently, GAO reported that out of 17 recommendations made by the VA Inspector General (IG), 16 had not yet been implemented. Implementing these recommendations is essential if the VA is to protect private information and meet its obligations under the Federal Information Security Management Act (FISMA).

In the final analysis, we must remember that IT is merely a tool, a tool used by the VA in furtherance of its mission of caring for veterans. This Committee has continued to work in a bipartisan fashion to encourage the VA to centralize its IT efforts. These efforts, we think, will lead to concrete benefits for both the VA, taxpayers, and most importantly, our veterans.

Our charge is to ensure that while VA is carrying out its mission, it does so with the best and most up-to-date technology that the 21st century provides, while securing that technology from outside manipulation and preventing improper disclosure of our veterans' confidential information.

We must at the same time foster creativity and innovation and the use of electronic medical records and other systems that have put VA at the forefront of medical care. These are not easy tasks. We are heartened by many of the steps the VA has undertaken, but remain concerned that more should be done, and could be done, at a faster pace.

We remain hopeful that the VA can simultaneously provide our veterans the greatest security, management, and healthcare. Undoubtedly, the efficient and effective management and operation of VA IT efforts will result in tangible benefits for our veterans.

I would yield for an opening statement to the Ranking Member of our Committee, Mr. Buyer. And you have 5 minutes.

[The prepared statement of Chairman Filner appears on p. 55.]

OPENING STATEMENT OF HON. STEVE BUYER, RANKING REPUBLICAN MEMBER

Mr. BUYER. Thank you very much, Mr. Chairman. First I would like to address the issue regarding the Vietnam Veteran's Memorial Wall. I was heartbroken to learn about the callous act of vandalism that resulted in the damage to the Vietnam Veteran's Memorial Wall on September 7th.

For every person that has ever stood before that wall, you can reflect upon your feelings and emotions as you stood before the 147 black granite panels. I could not help but sense and feel the humility of a grateful Nation and how small one feels standing before the granite.

What I will say publicly to the vandal is that you are nothing but a coward. These are cowardly acts to stand before that wall and to throw such a substance and attempt to deface the Vietnam Veteran's Memorial Wall.

The reality is that despite that act, you have no impact upon history. You have no impact upon the families who embraced their loved ones, that gave their lives for this country.

So to the coward, you can either step forward and accept responsibility for your act or forever crawl back under the rock from which you came.

Right now I would like to thank the Chairman. He and I worked together last year along with other Members of the Committee.

And I want to publicly thank Mr. Evans, in our efforts to centralize the IT architecture within the VA.

Mr. Chairman, I would like to thank you for responding to my request. More in particular, I compliment your timeliness in holding this hearing, with the exit and retirement now of the VA Secretary. I think it is just a wonderful time for us to get an update.

It is important for us to look back over the past year and see how the VA has implemented the instructions given in Public Law 109–461 and moved its IT infrastructure to a centralized model. This is the first step for any large, Federal department or agency of government.

We held a lot of hearings on VA's data breach, Mr. Filner. And so as we talk about the centralization of the IT infrastructure, it is also about security assurances. And I can't—when I think about the challenges that the Chief Information Officer (CIO) of the VA has, it is extraordinary.

And so while I compliment you, Mr. Chairman, for holding this hearing and getting the input, we also have to be cognizant of the task at hand and how long it is going to take to perfect a centralized model.

And patience is one thing that is going to be very hard for us to have, and for me in particular, because of my 7 years of interest in the issue. But I recognize how long it is going to take.

The goal of Public Law 109–461 was to provide the means to allow growth and development to move forward with a main central IT structure in which new, improved technologies and methodologies can be encouraged and shared throughout the VA. The new law also brought fiscal discipline to VA IT for the first time.

What I am interested in finding out today is how the centralized model is being implemented. And whether there has been any cultural resistance from local facilities toward centralizing.

I am also interested in learning what new technologies are being used. How will these technologies enhance the VA's ability to provide faster, better, and safer services to our Nation's veterans? What measures are being used to protect the identity of our veterans when they seek treatment or benefits from the VA?

I was very concerned when I learned about the 2006 Federal Information Security Management Act report being delayed and the VA receiving an incomplete in its FISMA reporting requirements. I trust that this will not occur again in 2007 reporting period.

I am also concerned about the continuing problems in IT security, which are detailed in the weekly Network Security Operations Center reports received by this Committee.

The Birmingham VA research breach involves more than a million Medicare and Medicaid providers. I would like to know how the IT vulnerabilities that we have seen in VA's research community are going to be addressed, so that incidents such as this no longer occur.

Last week, the GAO testified before the Senate Veterans' Affairs Committee and made 17 recommendations to the Secretary. Those recommendations aimed at improving the effectiveness of VA's efforts to strengthen information security practices by developing and documenting processes, policies, procedures, and completing the implementation of key initiatives.

For instance, why is the Veterans Health Administration's (VHA's) waiver for not encrypting physicians' laptops and other devices still in effect? I am looking forward to hearing the status of each of these recommendations from both the GAO and the VA.

Mr. Chairman, I would like to thank the witnesses for coming to testify before the Committee, and General Bob Howard who took the reins for the VA IT infrastructure during a wave of change.

I compliment you, sir. It is under his watch that the goals and policies set up by Public Law 109–461 are being implemented. And I look forward to hearing from you and continue to work with you.

General, I also want you to rely upon your military experience, because once you have made your advance, you have taken ground. And now that you have someone leaving, i.e., the Secretary, as an agent of change, other individuals are seeking to take ground back.

So you are going to have to defend. And I recognize that. And at the first moment, please pick up the phone, call the Chairman, call me. We want to work with you to make sure that you have the ability to implement the law.

And I would say to the witnesses, I had an opportunity last night to read your testimony. I have a Commerce Committee hearing on my other issue dealing with counterfeit drugs. And so I am going to have to excuse myself.

But thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Any other opening statements. Dr. Snyder? Mr. Walz? Mr. Brown? Mr. Lamborn?

All Members have 5 legislative days to revise and extend their remarks and all written statements will be made part of the record. Hearing no objection, so ordered.

Our first panel this morning is from the U.S. Government Accountability Office. Ms. Valerie Melvin is the Director of the Human Capital and Management Information Systems Issues Office. Mr. Gregory Wilshusen, is the Director of Information Security Issues. And accompanying you is Ms. Oliver. If you will introduce her, Ms. Melvin. Your written statements will be made a part of the record, so if you can keep oral remarks to about 5 minutes, that would be great.

STATEMENTS OF VALERIE C. MELVIN, DIRECTOR, HUMAN CAPITAL AND MANAGEMENT INFORMATION SYSTEMS ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; AND GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY BARBARA OLIVER, ASSISTANT DIRECTOR, HUMAN CAPITAL AND MANAGEMENT INFORMATION SYSTEMS ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF VALERIE MELVIN

Ms. MELVIN. Mr. Chairman and Members of the Committee, thank you for inviting us to discuss VA's information technology realignment and actions toward strengthening its information security program.

With me today, as you have noted, is Mr. Greg Wilshusen, GAO's Director of Information Security Issues, and Ms. Barbara Oliver, Assistant Director for VA IT issues.

In serving our Nation's veterans, VA relies heavily on information technology, for which it spends about $1 billion annually.

However, the Department has long been challenged in IT management, having experienced cost, schedule, and performance problems in its information systems initiatives, as well as security breaches that threaten to compromise sensitive and personally identifiable information.

To provide greater authority and accountability over its resources, VA is realigning its organization to centralize IT under the Chief Information Officer, relying on a defined set of improved management processes to standardize operations. VA began this realignment in October 2005 and plans to complete it by July 2008.

Over the past year, we have assessed and reported on the realignment. And just last week, as you noted, released a report on the Department's information security. At your request, our testimony today summarizes our findings in these two important areas.

In short, VA has made progress in moving to a centralized structure by fully or partially addressing all but one of six critical factors that we identified for a successful transformation such as this realignment.

Among its actions, the Department has ensured top leadership commitment to the initiative and established a governance structure to manage resources. However, it continues to operate without a single dedicated implementation team to oversee this important change.

And in addition, while improved IT management processes are a cornerstone of the realignment, VA has not kept to its timeline for implementing the processes and thus, has not made significant progress, having only piloted two of the thirty-six planned processes.

At the same time, VA has ongoing programs and system development initiatives that depend on effective management and use of IT resources, the essence of this realignment. Our recent studies have noted measures of progress in its efforts. But essential work remains, including addressing numerous and longstanding information security weaknesses.

Our report, released last week, notes that although VA has made progress in strengthening information security, much work remains to resolve its security weaknesses.

The Department has undertaken several major initiatives to strengthen information security practices and secure personally identifiable information, including continuing efforts to realign its management structure, establishing an information protection program, and improving its incident management capability.

Yet while these initiatives have led to progress, their implementation has shortcomings. For example, although a new security management structure exists, improved security management processes have not yet been completely developed and implemented.

In addition, this new security management structure divides responsibility for information security functions between two organizations, but with no documented process for the two offices to coordinate with each other.

Further, the Department has made limited progress in addressing prior recommendations to improve security that we and its In-

spector General have made. Although VA has taken certain steps, it has not yet completed the implementation of 22 out of 26 prior recommendations.

In summary, Mr. Chairman, VA is making progress on its IT realignment. But important work remains to ensure that effective management processes exist and that its IT programs and initiatives are fully and successfully implemented.

In our view, an implementation team and established management processes are crucial to the overall success of the realignment, without which the Department is in danger of missing its 2008 targeted completion date and of not realizing the potential benefits of this initiative.

Similarly, until the Department addresses the shortcomings in its IT security program, it will have limited assurance that it can protect its systems and information from unauthorized disclosure, misuse, or loss.

This concludes our prepared statement. We would be pleased to respond to any questions that you may have.

[The prepared statement of Ms. Melvin and Mr. Wilshusen appears on p. 57.]

The CHAIRMAN. Thank you. There are no other prepared statements from the panel?

Ms. MELVIN. No. This is our statement.

The CHAIRMAN. Thank you. And I appreciate you undertaking this. It has been very helpful.

Dr. Snyder, do you have any questions?

Mr. SNYDER. Yes.

The CHAIRMAN. Go ahead. I will wait.

Mr. SNYDER. I think you all make a great contribution in these areas.

I am always struck that somebody like us that can sit on these panels and, you know, make—we are prone to make accusatory comments about administrative agencies and their failures to do certain things.

I couldn't do this. I don't have the skills to do what we are asking the VA. Can you all do this? If you were plucked out and put in Secretary Nicholson's slot, could you do this, what you are asking this system to do?

Ms. MELVIN. Sir, this initiative is a complicated one.

Mr. SNYDER. Yeah.

Ms. MELVIN. It is one that from its inception, we have noted would take a lot of dedication. Was one in which VA was stepping out in a way that few other agencies have, in fact, done.

It is an effort that will require tremendous discipline, tremendous coordination, and exceptional communication on the Department's part to ensure that all of its management is involved, all of its users are adequately considered. That there is the necessary governance in place and the discipline process is in place to ensure that this can be undertaken.

Mr. SNYDER. Was that a no? Regardless of——

Ms. MELVIN. It means that it is a very complicated process that——

Mr. SNYDER. I think it is.

Ms. MELVIN [continuing]. Will require a lot of effort on the Department's part.

Mr. SNYDER. I think it is. I think the problem with it too is it is complicated. It is a challenge. And you outline, I think, some kind of hard attributes of the process. But it is about leadership, I think, and getting people to buy into it.

Did you—have you all looked at what the downside for veterans' healthcare is if these things are not being done?

Ms. MELVIN. Obviously, this overall initiative, it is in place so that the Department can have more effective processes for managing all of the initiatives that it is undertaking.

Certainly one of those, for example, is its veterans health information system. All of these initiatives are impacted by the efforts that are being undertaken and the sense that VA has previously operated in a centralized manner. And in moving—I am sorry, in a decentralized manner.

And in moving to centralization, it will be critical to make sure that the processes exist so that requirements can be understood effectively, identified effectively, and that solutions are in place to address them.

When you are looking at that, obviously there is the chance that if this is not undertaken properly, if it is not put in place in a discipline manner that allows all of the administration's IT needs to be addressed in a manner that supports the veterans, it could, in fact, impact veterans through the systems that are either put in place effectively or not put in place effectively.

Mr. SNYDER. I spent several hours sitting in an airport yesterday, because of something that happened with Memphis radar that shut down planes over several States. There was no—nothing—it was earlier at the Little Rock Airport. Nothing was coming in or going out.

And if you had asked us, I would think most of us would say well, there has got to be some redundancy in some system—in the system. We can handle whatever kind of technical problem. And yet,these kinds of things get so complicated that it can be—it can get so complicated it is difficult for a group of civilians here to provide that kind of oversight.

So we count on you all to do that for us. And I always struggle a little bit about what exactly do I think is the clear next step for them to take. What do I think they should be doing.

And it comes down to me as a matter of almost the personal leadership of the people at the top, the people that are at the highest position of leadership at the VA. This has got to be a number one priority, maybe second only to veterans' healthcare, or it is not going to get done.

Why I sometimes read these reports, they almost get so dry, which is I think what your approach is. That is what we want you to do. But that we forget about the dynamic leadership that can make this kind of thing occur through a big system.

Thank you for your contribution. I don't have any further comments, Mr. Chairman.

The CHAIRMAN. Thank you. Mr. Stearns.

Mr. STEARNS. Thank you, Mr. Chairman. I sort of tend to think that we can solve this problem. General Motors, a large corpora-

tion, is able to keep track of their security. They set up a security database with a security chief officer. They are able to coordinate with all the plants, not just in the United States but around the world.

IBM, as I understand, is a subcontractor to you folks. And IBM has been successful in setting up internally their own IT network.

So I don't think it is without the realm of possibility. In fact, if the private sector came in and did this, wholly I suspect they could get it done.

I think Dr. Snyder's probably correct, it is one of leadership. But it also inherently difficult with bureaucracies, because it has been decentralized. And these bureaucracies are not talking to each other. But I am optimistic that you can get it done.

In May 2006, VA experienced the largest data breach in the history of the Federal Government. In January 2007, VA Birmingham, Alabama, suffered a breach of unbelievable magnitude involving any practitioner that has ever billed Medicare or Medicaid.

My question is, is the VA data at risk today? Notwithstanding where we are, is the VA data at risk today? Can you tell me "yes" or "no"?

Mr. WILSHUSEN. Yes, it is, sir.

Mr. STEARNS. And is that agreed by all three of you? Was that pretty much the unanimous consent of all of you that the VA data is at risk?

Ms. MELVIN. Based on my understanding of the work that Mr. Wilshusen has done, I would say yes.

Mr. STEARNS. Now, Mr. Wilshusen, why don't you explain why you think it is at risk?

Mr. WILSHUSEN. Okay, certainly. First of all, I would like to note that VA has made important progress in improving its information security practices and policies. However, much more needs to be done.

For example, VA has not yet fully implemented two of our four prior recommendations, including one to complete a department-wide information security program.

In addition, it has not yet fully implemented 20 of 22 recommendations made by the Inspector General (IG) with regard to improving information security.

For example, it has not yet completed the activities to appropriately restrict access to its information, computer systems, and networks. It has not yet implemented appropriate physical security safeguards to protect its information technology resources and facilities, nor has it ensured that all authorized—that only authorized changes and upgrades have been made to computer programs.

Until these recommendations are implemented, unnecessary risk exists that personal information of veterans and others, including medical providers, such as—or such medical providers, will be exposed to data tampering, fraud, and unauthorized or inappropriate disclosure.

Mr. STEARNS. Based upon what you said, would you be willing to track the VA's progress in implementing their consolidation plan and report back to us on a regular basis?

Mr. WILSHUSEN. Yes, we would. Yes, I would.

Mr. STEARNS. What are the short-term, mid-term, long-term consequences and vulnerabilities for the delay in VA's integration and consolidation plan? And I guess—go ahead.

Ms. MELVIN. In terms of VA's centralization, the concerns that we have relate to the extent to which the Department implements the critical processes that it has identified for this initiative.

The Department has identified 36 processes that are critical or the foundation I should say to the overall—having an overall discipline process in place that allows it to oversee and account for its IT investments.

In the immediate, we noted that the Department has, in fact, put a governance structure in place, so that they have some immediate levels of responsibility.

However, in looking out over the initiative as it continues to carry out this implementation, we have concerns from a longer term relative to how they are actually—or the progress that they are making, I should say, in actually fielding the leadership for the positions that it has. The extent or the time frame in which it would get its management processes in place.

At the same time that the Department is undertaking this realignment, as I mentioned in my statement, its systems development initiatives and programs are still being undertaken.

So in the long term, having this system in place and having it in place the sooner the better relative to its impact on the overall initiatives that it is undertaking and how effectively it can continue to move forward with those project for systems development.

Mr. STEARNS. Have you seen any bureaucratic or cultural push back toward this implementation in the administration?

Ms. MELVIN. We have heard through our assessment that there has been concern from the clinicians, for example within the Veterans Health Administration, that in doing this, some of their innovation will be stifled.

And I think this is driven by their past experience in the initial—the development of the initial VistA system. However, what we have stated through our work is that if the Department is able to move forward and maintain momentum in terms of having an effective communication strategy in place, having the overall leadership in place relative to the many offices that it has identified.

For example, they have identified 25 offices that are being put in place to implement and execute the 36 management processes that will give it a disciplined approach to managing its investments and resources.

However, at the time of our review, those—not all of those offices had been filled. I think it is somewhere in the range of probably 15 or more either had not been filled or had been filled only in an acting capacity.

Our concern with that is that without the stable leadership, the Department does not put itself on a solid and a sustainable foundation for being able to carry through with the realignment itself. And then certainly to execute all of the processes that are necessary to carry out its investments and its projects.

Mr. STEARNS. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Mr. Walz, your witness.

Mr. WALZ. Thank you, Mr. Chairman. And thank you to each of you for being here. It is a very important service that you provide. And every time we testify in this Committee, I think it is very important for us to always remember the ultimate goal here is the service to our veterans and making sure that is possible.

And I think I associate myself with Mr. Snyder—Dr. Snyder's comments on this. It is all too easy to point fingers at this. And this is a—this is a large task.

And I also associate myself to a certain degree with my colleague, Mr. Stearns, that I believe this can be fixed. Although his faith in the private sector, seems to forget the letter that I received in June of 2005 when my MasterCard data, along with 40 million others, were compromised.

So it cuts both ways. It is a difficult task. But it is one that I think we are hitting on, and some of the questions got asked. But I just have two questions that I am concerned about.

I represent the Southern Minnesota district that includes the Mayo Clinic. And I have had a lot of talks on this issue, on the VA side of things, on the quality of the VistA system and their medical records, which is arguably the best in the world.

My concern is, and you hit on it to a certain degree, do you have a concern that any of this is going to be the movement forward we have had on the VistA system, the electronic medical records, and our push to seamless transition with the U.S. Department of Defense (DoD) is going to be affected by this realignment? If you could comment on that in your opinion.

Ms. MELVIN. Obviously, in undertaking the realignment, the key will be making sure that the Central Office of Information and Technology, which is the key point at which the centralization is taking place, is in touch, if you will, with the administration, in this case the Veterans Benefits Administration (VBA). I'm sorry, Veterans Health Administration.

And what we have seen in our work and what we have advocated through the success factors that we have emphasized as a part of our most recent study, was the need for the Department to have adequate communication and a balance relative to ensuring that the requirements, the needs of the administrations, are adequately identified, heard, and dealt with as a part of the overall efforts that are undertaken.

Obviously, that means that the Department has to get in place its main office that is identified to serve as the conduit of communication between the administrations and the central office.

At the time of our assessment, that office had not been staffed and its leadership had not been put in place. So we view that as critical to making sure that they have the necessary balance for making—for ensuring that administration needs are identified, that solutions are identified to address those needs, and that there is a necessary follow up to ensure that the delivery takes place in terms of services provided through the IT that the central office supports.

Mr. WALZ. And my—just my final question here. And this is I guess a bit more subjective. I come from—my background is in cultural studies and this issue of culture or what is there. I know

when the issue came out of the data breach, I also received a letter on that as a veteran for my data breach.

And it seemed like at that point though there was a slowness to it, a reluctance to move on this. Do you get a feeling, and this as I said is very subjective? I have complimented many of the Members who have taken over on this in a very difficult time.

And I feel that there is a—maybe there is a shift in the culture of understanding this. And I am convinced that this is central before we can move forward, if they really understand that. If you may—if you could comment on that.

Ms. MELVIN. I would agree with you. Definitely key to this is the cultural transformation that is necessary, along with the actual implementation of new processes.

Key to that, again, as I have mentioned earlier, is communication. We do feel that that is one of the critical aspects that has to take place. In our work, we found that the Department has taken some efforts toward trying to improve its communication in dealing with the administrations.

But there is still more work that can be done through ensuring, as I mentioned earlier, that its business relationship management office is staffed up. That the necessary individuals are in place in positions there to serve as the conduit of communication, through actual information sharing and making sure that the users understand what it is that the Department is trying to accomplish and how they plan to do that. And the impact of how that change to centralization will affect the Department from the standpoint of identifying business requirements, addressing the requirements.

Only until they have had an opportunity to really communicate and reach agreement and understanding on those aspects will there be a cultural change, will there be what I would say is more user buy into this overall initiative.

Mr. WILSHUSEN. And I would just add from an information security perspective that the tone at the top has increased significantly with regard to taking corrective actions to implement effective security controls since the May 2006 data theft.

I think that was a watershed event, which really caused and highlighted the need for strong information security control. And we have seen a shift throughout the entire organization in the terms of—particularly with reporting incidents of potential data breaches or loss of information. Just prior to and subsequent to that May 2006 event, for example, the number of reported incidents doubled over the 5 months following it, versus the 5 months preceding that point.

In addition, the number of initiatives that the VA has undertaken to improve security, and they are making progress. Many of them have not yet—many of those initiatives have not yet been completed. But they are taking steps to implement stronger controls.

Mr. WALZ. Great. Well I thank you. I yield back, Mr. Chairman.

The CHAIRMAN. Mr. Brown, any questions?

Mr. BROWN OF SOUTH CAROLINA. Thank you, Mr. Chairman. And thank you to the witnesses for coming this morning. I know this is a major concern of mine and of course of all the veterans around the country.

Do you think we are—we are better off today than we were back in 2006?

Mr. WILSHUSEN. With regard to the——

Mr. BROWN OF SOUTH CAROLINA. Security.

Mr. WILSHUSEN [continuing]. Security of——

Mr. BROWN OF SOUTH CAROLINA. Right.

Mr. WILSHUSEN [continuing]. Their personal information, I believe VA has taken steps to improve information security. And these steps include encrypting the information on thousands of laptops, initiating a remedial action plan to identify and to take corrective steps to improve the security controls, but much more still needs to be done.

There are still significant and unnecessary risks to veterans' information. But I believe that they are taking steps in the right direction.

Mr. BROWN OF SOUTH CAROLINA. Do we have a system in place that we can identify if there is a breach at some point in time?

Mr. WILSHUSEN. Well there are technical controls that are available to look for and to detect anomalous behavior and whether or not there have been breaches, if you will, or intrusions into the systems in networks of VA.

VA, I believe, is in the process of acquiring and installing intrusion prevention systems on various devices that will help prevent and to detect such occurrences.

Mr. BROWN OF SOUTH CAROLINA. Well I believe in the past we have had like people taking their laptops home and this sort of thing. So I was just trying to——

Mr. WILSHUSEN. That is correct. And that is why the physical security controls and the use of encryption on portable media and laptops is so important, because you correctly state that many of the or several of the most significant security breaches were the result of physical theft of equipment.

And so it is important that VA first inform and train their staff on what the proper controls are over that equipment and over that information and to put in the appropriate controls to prevent them from occurring.

Mr. BROWN OF SOUTH CAROLINA. And how long do you think it will take to implement a system that we can feel comfortable with that our records are secure?

Mr. WILSHUSEN. VA, in its remedial action plan, has identified over 400 action items in which it is undertaking to improve various different aspects of information security.

Some of those actions extend out to June—or I am sorry, out to 2009. Even upon completion of those actions, many of which are to develop or update a policy or procedure, the true test of determining whether or not the agency has effective information security controls is whether or not they effectively execute those policies and procedures.

And, as my father once told me, and I am paraphrasing him now, "The road to insecurity is paved with good intentions." And developing policies and procedures shows what the management's intentions are with regard to securing information.

But it gets down to the detail of actually implementing those on a sustainable, ongoing and consistent basis throughout the organization.

Mr. BROWN OF SOUTH CAROLINA. We don't recognize the cultural education we must perform. Is there anything that we can do as Members of Congress to help expedite that process?

Mr. WILSHUSEN. Well, one, the passage of the Veterans Benefits Healthcare and Information Technology Act of 2006, I think, was a positive step forward. And in addition to holding these types of hearings, holding VA officials accountable for their actions and maintaining a dialog with them, with you and your staffs with the VA officials to assure that appropriate actions are being taken.

Mr. BROWN OF SOUTH CAROLINA. Thank you very much.

Mr. WILSHUSEN. You're welcome.

The CHAIRMAN. Ms. Herseth Sandlin.

Ms. HERSETH SANDLIN. Thank you, Mr. Chairman. Thank you for your testimony today. I would like to pick up a little bit where Mr. Stearns had asked your willingness, GAO's willingness, to track the VA's progress and report back. And you had answered "yes." And I appreciate that.

But let me ask you this, I assume that in doing that, your job would be easier if the VA would actually dedicate an implementation team to manage the change, so that you had a team you were directly working with, which is the team within the Department that's supposed to be tracking the progress and managing the change.

So could you confirm for me that the VA has not yet acted on that critical success factor?

Ms. MELVIN. As it pertains to the realignment initiative, the VA has not put what we would desire to see in terms of a single dedicated implementation team to manage that overall effort.

It does have multiple offices designated to oversee the realignment effort. Our concern is that there is not a single body that is dedicated to ensuring that there is the necessary oversight for the—managing, for example, the schedule against goals and timeframes for accomplishment. Identifying shortfalls and being able to ensure that there is a consistent coordination throughout the Department relative to how these are handled.

We feel that it is important also in terms of having some consistency through leadership changes that occur so that the Department has a voice that speaks for the overall realignment. And that ensures, from an oversight perspective, that it is occurring as it should.

Ms. HERSETH SANDLIN. So I think you answered my other question. There is no timetable other than the July 2008 date upon which this is to be completed. But there are no quarterly objectives. There is no, as you said, single entity in place to help set the objectives, track the progress.

What has been the Department's reaction to your concern about the lack of that type of entity that would help effectively manage the transformation?

Ms. MELVIN. The Department has stated that it is taking some actions, for example, toward business processes in terms of identi-

fying timeframes. And they prioritized some of those. But we have not seen specific dates attached to those.

But when it comes to the realignment team in and of itself, the Department has effectively stated that it would agree to disagree with us on the need for a single dedicated team.

They have not indicated that they wouldn't have multiple teams working. But, again, our desire would be to see a single dedicated team that can ensure a coordinated oversight for this initiative.

Ms. HERSETH SANDLIN. Well, Mr. Chairman, I would just suggest that in light of the Secretary's resignation, and of course our continued hope that there is the tone at the top with the Under Secretary's, the deputy assistant secretaries, to improve the system.

I actually think that given the transition here, the lack of stable leadership at the top. And I do think Secretary Nicholson, working with this Committee, working with the Ranking Member, working with Committee Staff last year when this problem presented itself and how we go about the information security objectives, I was very committed to it.

My concern is the transition. And so I think it highlights the importance of a single dedicated board, governance board, within the VA in light of that transition. And would hope that with our oversight that we can, with the testimony we will be hearing from the later panels, continue to work with them to—if you would agree.

And if the Ranking Member and Mr. Stearns and other Members of the Committee agree with the GAO assessment as I do, that a single dedicated entity is of the utmost importance in helping manage the transformation that we work through our oversight and our discussions with the VA to see that that would happen to try to stay as on top of the July 2008 deadline as possible.

And I would yield back.

The CHAIRMAN. Thank you. Just to follow up, I mean, when you say you have agreed to disagree, is there a reason? What is their reason?

Ms. MELVIN. I think they can best answer that. But in talking to them through our assessment, they feel—felt strongly that the offices that they are putting in place, and they have identified two specific offices, they feel that those offices are capable of providing the necessary oversight and coordination for this effort.

Our concern is that this is an extremely large initiative that involves many processes, that involves many layers of management and the need for solid and extensive communication throughout the organization. And certainly established timeframes that can be monitored closely and that the organization have some consistency in how it measures and tracks performance toward achieving its overall goal for 2008.

The CHAIRMAN. And of the two major teams, one of them is—its top position is vacant, right?

Ms. MELVIN. Yes, that's correct.

The CHAIRMAN. Thank you. Mr. Bilbray.

Mr. BILBRAY. Thank you, Mr. Chairman. You know, Mr. Chairman, all the concerns about the information systems kind of reminds me of the fact that ever since man started messing with technology, there has been a fear of it, and a threat of it, and, obviously, an opportunity.

I mean, fire would be a good example. I think that there are a lot of people in Washington if they had been the caveman with the first fire, it would have been outlawed, restricted, and banished from the world.

I think the keys we are looking for though is that we first of all needed something that is expandable and transformable. It has got to be able to adapt to the situations.

And actually the Chairman and I went through years in local government working the same issue, the city of San Diego, trying to work out emergency response information systems, the county doing the same thing. And Mr. Chairman, I would just like to let you know that though you worked hard at the city, the city now has accepted that the county system is so much more effective and is adopting that system for their emergency information system. To have—I can't pass up the chance to take a cheap shot.

My question to you though, the laptop situation was sort of interesting. With all the encryption on there, wouldn't it be so much more secure if with these mobile information modes, that only the person who is authorized to use that or who supposedly has it delegated to them, if the technology was there to where only they could activate the system, wouldn't that be even a step further in securing the information of the veterans?

Mr. WILSHUSEN. Yes, it is. Certainly that would be like the first step in protecting sensitive information is to make sure that only those individuals who have a legitimate business need for access have access.

And once that is granted, then to have other controls to enforce that level of access. And then also to protect the information such as using encryption and other technologies to protect it—while it is being stored on laptops and other devices.

Mr. BILBRAY. How many of our mobile and how many of our stationary now are going or do have biometric access control systems?

Mr. WILSHUSEN. I don't know the precise number in terms of how many of the laptops or other devices have biometric capabilities on them at VA.

Mr. BILBRAY. Many laptops have as an option biometric access that have had it for over a decade. And after what happened with the laptops, I just think it is almost like any businessman would say we are going to go to this option now, just as a matter of fact.

And I would really challenge, if we haven't done it, why we haven't done it. And really look at the fact that here are those simple little things that the private sector would be doing at the snap of a hat. But we are always lagging behind in the hope that we will go over to that.

I mean, frankly, I don't know of a major manufacturer of a laptop who does not provide the option that a thumbprint can be used as the primary access before the machine would even turn on. And I would sure like to see if we are moving forward with those little things that can really make a difference.

If somebody steals a laptop and can't even turn the thing on, that is even better than encryption control.

I yield back, Mr. Chairman.

The CHAIRMAN. Thank you. Mr. Hare.

Mr. HARE. Thank you, Mr. Chairman. I apologize for getting here a little bit late. I had another meeting. So if you have covered these, I hope you will bear with me. But I am just interested in the answers that you might have here.

What are the main reasons that you found for lack of a single integration team to oversee this implementation?

Ms. MELVIN. The main reason was that the Department, as I mentioned earlier, just felt that it had the necessary offices in place to carry out the oversight and monitoring of the implementation.

But, again, as was stated previously, one of those offices is vacant at this time. And our concern is that with the magnitude of this overall effort, there is a need for a coordinated oversight through a single dedicated implementation team.

Mr. HARE. Do you think there is a correlation between the lack of staffing in these key leadership positions and the delay in establishing the management processes?

Ms. MELVIN. I think it is certainly—if it has not had an impact, will have an impact on the Department's ability to meet its timeframes for getting the processes in place. The individuals that it has identified and the offices that it has identified are the ones that are supposed to implement and execute these processes.

The Department has acknowledged that they are behind in doing that. But we do feel strongly that it is important to have the staff there to carry out the processes or you are unlikely to have a disciplined approach to managing the investments and resources.

Mr. HARE. What other hitches do you think—what are the other hitches that are causing the delay in developing the 36 management processes?

Ms. MELVIN. I am sorry, what are the delays?

Mr. HARE. What other hitches are causing do you think——

Ms. MELVIN. The issues that are causing it?

Mr. HARE. Uh-huh.

Ms. MELVIN. What—in talking with VA's management, we were told that—and quite frankly they do recognize that they are behind in implementing the processes. What they identified were some concerns relative to really the definition of the processes that the contractor recommended for them. And the need to redefine and reassess what those processes were relative to their offices in place.

Also they identified the need to really look at the processes relative to responsibilities and ensuring that they clearly discerned which offices would be responsible for key activities under those processes.

And in some cases, they are still clarifying who has key responsibilities. The Office of Information and Technology won't have full responsibility, for example, for all of the financial management processes, as the Department has an office of management that oversees its overall budget. So they are working through those issues.

And then as you mentioned earlier, a key concern of ours was the—that the 25 or so offices that they have identified to implement and execute the processes have not yet been fully staffed and don't all have full leadership to direct them.

Mr. HARE. Have they indicated when they would be staffed?

Ms. MELVIN. When they will be staffed?

Mr. HARE. Mm-hmm.

Ms. MELVIN. We did not get information on when they would be staffed.

Mr. HARE. Okay.

Ms. MELVIN. They did indicate that they were looking into the staffing. That they saw this as a difficult process that they would need to work through.

Mr. HARE. Thanks. And my last question is how much collaboration and communication did you find that there is or is not between the two implementation teams?

Ms. MELVIN. I believe that the implementation teams are collaborating with one another. I don't think our assessment looked fully at exactly how all of the collaboration is occurring.

We do maintain, however, that there has to be collaboration across those. And it has to be extensive relative to the processes, relative to the overall staffing of the offices that need to take place.

Again, however, from our standpoint, we would like to see more assurance that there is the necessary coordination that would be gained through having a single devoted body to overseeing this effort.

Mr. HARE. Okay. Thank you very much. I yield back, Mr. Chairman.

The CHAIRMAN. Thank you. Ms. Brown-Waite.

Ms. BROWN-WAITE. Thank you very much. I had votes in Financial Services. And that is why I was late.

I don't care which one answers this. And you may or may not have the information with you. But I understand the VA says that they have encrypted 16,000 laptops. Is that correct?

Mr. WILSHUSEN. I am not aware of that particular number. But they have an initiative underway where they are encrypting thousands of laptops. I don't know if 60,000 is the correct number.

Ms. BROWN-WAITE. No, 16.

Mr. WILSHUSEN. Oh, 16.

Ms. BROWN-WAITE. That they have encrypted——

Mr. WILSHUSEN. Okay.

Ms. BROWN-WAITE [continuing]. 16,000, which brings me to the other part of my question. If it is 16,000, that is out of how many laptops that the VA has?

Mr. WILSHUSEN. Well——

Ms. BROWN-WAITE. Do you——

Mr. WILSHUSEN [continuing]. The total number of laptops, I don't have that information. But I do know there is a sizable number of laptops that have not been encrypted. Many of these are being considered medical devices.

And right now the VA's policy is not clear as to which devices or laptops should, in fact, be encrypted. And that is one of the recommendations that we are making that they clarify that policy.

Ms. BROWN-WAITE. So medical information may be out there without encryption. Is that what you are——

Mr. WILSHUSEN. That would be the case.

Ms. BROWN-WAITE. Okay, another question. There are many instances where there are laptops not owned by the VA but used by VA personnel, and/or perhaps contractors, or the VA research communities. Are they still unencrypted?

Mr. WILSHUSEN. I don't know. Our assessment did not look at the encryption of non-VA equipment. But if individuals or contractors have sensitive Veterans Administration information or sensitive veterans' information on them, on behalf of VA, those laptops should be protected to the same level as required by VA.

Under the Federal Information Security Management Act, VA is responsible for assuring that the systems and equipment that are being operated on its behalf by others, should be protected to prevent and protect against unauthorized use, access, and disclosure of information.

Ms. BROWN-WAITE. Let me ask another question. There is a program out there that you can buy. It is called "Go to My PC." If a VA employee is at home and uses this kind of a "Go to My PC," and there may be confidential information on their personal computer (PC) at the VA workplace, can they gain access to their PC in the VA workplace from a remote location?

Mr. WILSHUSEN. Well I am not familiar with the specific program, but—that you mention. But certainly implementing appropriate controls over remote access to VA information on VA devices is a consideration that VA needs to address and implement appropriate controls. Obviously, there are a number of individuals within the VA community that do access information remotely. And assuring that those—that VA has implemented remote controls is very important.

Ms. BROWN-WAITE. And you have brought this to their attention?

Mr. WILSHUSEN. We and the Inspectors General. One of the vulnerabilities to VA systems is the access to data systems and networks. And that is a vulnerability that has been long standing in nature. And VA is taking certain actions to help improve its network security. But those actions are still on going and underway.

Ms. BROWN-WAITE. Thank you very much. I yield back the balance of my time.

The CHAIRMAN. Thank you. And, again, thank you for your report. You know, we talk with regard to the Iraqi War about benchmarks. And I couldn't imagine anybody doing worse than our government in meeting those benchmarks in Iraq. Except now you have an agency that has done even worse.

As I read your report, out of the 36 management processes that were set out to have been completed, out of the 17 recommendations of the Inspector General, one has been completed.

I am amazed. Here we are, almost a year and a half after this crisis. And it is as if once the crisis passed, everything goes back to normal. I still don't understand the lack of progress on this. It is as if well, you know, we have had our hearings, so they will forget about it. And we don't have to do much.

Again, I don't know what the reason for it is. You talked about 25 or so key positions to deal with this. And you estimate around 15 are vacant. Two implementation teams that have split responsibilities. Security still a major concern.

I mean, if you had to summarize the reasons for this lack of progress, how would you do so? Is it lack of leadership? Is it lack of resources? What is going on here that we are, a year and 4 months or 5 months after this incredible problem and we haven't made very much progress it sounds like?

Ms. MELVIN. I would start by saying that the Department's top leadership has certainly committed to this particular effort.

What we found, I think, when we look across VA and our work over the agency in the past times, one of the things that we have noted has been just overall project management as being an issue that the Department has to deal with. It is something that they have grappled with over time.

In this particular case, again, I would say that, you know, this is a very complex effort. It does require a lot of coordination. It does require a lot of communication on the Department's part.

And I think in terms of the actions that they are taking through their overall project management steps to lead this effort and to guide it through, there have been things that the Department needs to still address. Certainly in getting its leadership in place, knowing what resources it has, and to make sure that those resources are there to help it carry through with the implementation until they get some of those basic processes for communication, for leadership addressed and the staffing in place, the Department is at risk that it won't be able to get its disciplined approach in place through the 36 processes that it still has to implement.

The CHAIRMAN. Well, it may be complex. But this is not rocket science. And Mr. Stearns said it. These are rather ordinary problems that every company faces every single day in our society, every Nation faces it.

Has the VA used consultants from the private sector on all this? They must have. If I were the Secretary or the President, of course we would be better off if that were the case, I would call in Bill Gates or somebody from Microsoft and say, "Look, as your contribution to the national security of our Nation, fix this for us as a donation." I am sure they would do it. I think in 90 days they could solve this problem.

Mr. STEARNS. Bill Gates could probably——

The CHAIRMAN. Yes.

Mr. STEARNS [continuing]. Bring in his team. I can't resist, Mr. Chairman. Are you recommending immediate withdrawal?

The CHAIRMAN. From Iraq or from the VA?

Mr. STEARNS. The VA.

The CHAIRMAN. Immediate redeployment.

Mr. STEARNS. Redeployment, okay.

Ms. MELVIN. Mr. Chairman, in response to your comment, I would state that during our assessment, where we saw the Department's realignment contractor very much involved with this effort and taking a dedicated stand relative to helping the Department define its processes and get to a certain point, we did feel that the Department was making progress on this effort. Our concern is as the Department continues to move forward, that it has the necessary leadership in place, that it has the necessary staffing and communication in place to sustain the effort to not backtrack, if you will, through not having a coordinated oversight for this effort.

So we have seen some progress in the past. But certainly we would agree that there is a tremendous amount of effort that is still necessary. And it does take sustained and dedicated leadership oversight, accountability, and appropriate communications to make that happen.

The CHAIRMAN. Mr. Stearns has suggested shock therapy to this—to the culture. And I guess we want to know what kind of shock can we administer?

Mr. STEARNS. What could we as the Members of Congress here do? I mean, we are asking some very difficult questions. And we are sort of frustrated, as you can expect here. What could we, as Members of Congress, do to sort of expedite this?

You are alluding to the fact that this culture is—everybody is protecting their own turf. And this bureaucracy is so immense that no one can get through it.

We don't even know how many laptops there are. So if you don't know how many laptops there are, you don't have any idea how big the problem is.

So considering what the GAO found, Chairman Filner's correct. Two of six critical success factors identified as essential to successful transformation have been accomplished. But that leaves four that have not.

And as mentioned earlier, 22 of the 26 recommendations from the Department's Inspector General have not been implemented. So only four have.

And it goes on to even caution its limited assurance that it can protect its system and information from the unauthorized disclosure, misuse, or loss of personal, identifiable information. I mean, that is a pretty strong statement.

And here we are frustrated, because we have been having hearings on this. We talked about it. And so, I mean, is there anything that the U.S. Government elected official should do that we are not doing?

Ms. MELVIN. I think beyond the oversight, that you should continue, obviously, there is room for looking at particular cases in terms of how VA actually implements this process.

And really perhaps taking—making some dedicated case studies, if you will, of how this effort really plays out and the impact of the realignment efforts on key initiatives that the Department might be undertaking would be an approach to really getting a handle and a good feel for just how effectively the realignment is being executed.

Mr. STEARNS. Thank you, Mr. Chairman.

The CHAIRMAN. As you heard, there are bells for votes that we have to take. Just two votes. So we are going to have to recess. We do appreciate the expertise of the GAO in this matter. We would ask you not to be shy about recommending things that we might do in the future.

And I will say to the next panel, which is the VA, you are going to have now 20 minutes before we get back here. Throw away your prepared remarks. And deal with these questions in a candid way.

I mean, what is going on with all these vacancies? Why can't, if Mr. Bilbray is right, a simple thing like biometrics be used? Why has there been slow implementation of all these recommendations? What is your reason for these two implementation teams? Why is security still a risk?

These are questions that every veteran has assumed that we had taken care of after the crisis. And they—we are the representatives

of those veterans for assuring them that. And now it turns out we can't assure them that that is the case.

So I would like you to address those issues in just a common sense way without hiding behind all the bureaucracy. And let us have a conversation when we return in about 15 minutes for the second panel.

Thank you so much for the——

Ms. MELVIN. Thank you, Mr. Chairman.

[Recess.]

The CHAIRMAN. We will continue this meeting of the House Committee on Veterans' Affairs and move on to panel two who we thank again for their contributions to this discussion.

We welcome Assistant Secretary for Information and Technology at the Department of Veterans Affairs General Howard. And Mr. Claudio is the Executive Director for the Office of IT Oversight and Compliance.

To summarize what I had said earlier, Mr. Howard, you are a General. Just give the orders and make it happen. You are on.

STATEMENTS OF HON. ROBERT T. HOWARD, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND CHIEF INFORMATION OFFICER, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND ARNALDO CLAUDIO, EXECUTIVE DIRECTOR, OFFICE OF IT OVERSIGHT AND COMPLIANCE, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY ADAIR MARTINEZ, DEPUTY ASSISTANT SECRETARY, INFORMATION PROTECTION AND RISK MANAGEMENT, OFFICE OF INFORMATION AND TECHNOLOGY; AND CHARLES DE SANNO, ASSOCIATE DEPUTY ASSISTANT SECRETARY OF INFRASTRUCTURE ENGINEERING, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF ROBERT T. HOWARD

General HOWARD. Sir, you had mentioned earlier that you didn't want me to give an opening statement, so we can dispense with that. You mentioned earlier not to give an opening statement so——

The CHAIRMAN. No, I just——

General HOWARD [continuing]. I dispensed with that.

The CHAIRMAN. However you feel you can—you want to deal with this.

General HOWARD. Okay, sir.

The CHAIRMAN. I was just making a suggestion.

General HOWARD. Yes, sir. There are two other individuals at the table with me this morning, sir: Adair Martinez is my Deputy Assistant Secretary for Information Protection and Risk Management, and Charlie De Sanno to my far right is the Director of Region IV and also Infrastructure Engineering. So they are here with us as well.

I will read my testimony. I can get into addressing the issues as you requested. And first, sir, I don't know if you noticed or not, when you were giving your opening statement, I had to leave the

room and my apologies for that. I had to take a phone call from the Secretary in fact.

Sir, where would you like me to begin? I think perhaps a good start point would be the issue of the processes, because, obviously, that was an issue that the GAO was concerned about, and a number of the Members were concerned as well.

And so I would like to comment a little bit on that. First of all, as stated by the GAO, you know, we realize the importance of these processes. There is no question about that.

But they are right. We have—we have not been as speedy as we would like in implementing those. There are reasons for that. I am going to cover some that we are well on the way on.

But one of the reasons that has delayed us to some degree is this, we created the organization. We moved 6,000-plus people in all of that. We have a new appropriation. You know, we have things in place now to help make this happen.

But what we have also inherited are the problems that were out there. And there are a number of them. And those have moved right up in priority.

A good example of that is asset management. You know, the Oversight Committee had a hearing on that a few weeks ago. That is a real problem. We have had to put a lot of energy on that.

And so my leaders, and I will get to who they are in just a minute, are putting a lot of heat on them to fix a number of problems that we have uncovered, because what the organization has done, in addition to a number of things, it has made more clear, you know, what is going on within the VA with respect to information and technology.

It has also provided us better control, you know, over fixing these things. And you are right, we are not there yet. We have a lot of work to do. And, obviously, the control over the appropriation is also very helpful.

But this issue of visibility has caused us to see a number of problems that must be fixed. We have seen, for example, that we have the haves and the have-nots. There are some activities within the VA that have paid attention to information technology in the past and stayed up to date and all of that. And there are others that have not. You know, in a decentralized operation, if you are a director of a facility, it is up to you, you know, where you spend your money and where you apply the emphasis.

And there is a mixed situation out there right now. And you know one of the goals of our organization is to try and standardize that.

And so focusing in on the problems has definitely caused a slowdown in the implementation of some of these processes.

However, with that said, let me address a couple of issues. First of all, the one issue that we disagreed with the GAO is establishing a group to make this happen. We—I disagreed with that, because quite frankly, my military experience, you know, we have—we have a number of Deputy Assistant Secretaries. I have five of them in fact that are responsible for certain areas.

And we want those individuals to implement these processes, for example, my Deputy Assistant Secretary for Information Protection and Risk Management, Adair Martinez. There is a process that we

must implement called incident response. This is in her area. She has got to do that. She is going to implement that, and gain ownership of it, be responsible for it, and all of that.

If you look at the—all the way over to enterprise operations and infrastructure, you know, where Charlie De Sanno happens to be located, there are a number of processes that have to be implemented there.

Let me give you a perfect example. They are called SLAs, service level agreements. We have had a number of meetings so far in trying to hone in on what is the service level that we agreed to, you know, with the customer? Those have to be adjudicated. You know, how long does your computer stay up? The pane screen, you know, pane on the screens and all of that. The password timeouts, and what have you, all have to be agreed with. Downtime, you know, what are we on the hook for with respect to downtime.

These are service level agreements where discussions have already taken place. There are two additional offices though. So by and large, my key leadership, the monkey is on their back, you know, to implement processes that are in their areas. And we have divided that up. Each one of my Deputy Assistant Secretaries knows of the 36 processes. Thirty-six processes, they know the ones that they are responsible for.

In addition to that, we actually do have an organization called Organization Management. It is the remnants of the team that actually formed the reorganization itself. That box is still there. Unfortunately it is empty. The individual left about a week ago. But I intend to fill that. I do need someone as my conscience, if you will. I don't necessarily need them down into the weeds, you know, doing all of the detail. But I do need someone. So that part of it that GAO came up with, I don't disagree with.

Now in addition, we have a Quality and Performance Office. The individual in charge of that office right now is Martha Orr. She handles the monthly performance reviews and what have you. The focus for processes, the focus for all 36 processes is out of her office.

Again, she is not responsible for implementing each one of them. But she is responsible for coordinating the activity to keeping our eye on how these are going and what have you.

The CHAIRMAN. You may be getting there. But I didn't hear the word "timeline" or, you know, "goal"—a timeline for any of this or a goal. And the problem I always have with the word "process" is that a process is always ongoing.

General HOWARD. Yes, sir.

The CHAIRMAN. What about the results? What are we getting out of this process, and when is the timeframe within which we are going to do it?

General HOWARD. Sir, let me focus in on a couple of them. SLAs, service level agreements. In fact, just several days ago the individual in charge of that briefed me on his timeline.

And, you know, I can't recall the exact dates. But it is somewhere in the November, you know, end of November, end of October, beginning of November timeframe to come to agreement, you know, with VHA, with VBA, on what these are and then start implementing them.

And, in fact, some of them are already implemented. Particularly in—like for example, in region four. So there are timelines associated with some of those. And that one is an example.

Incident response, sir, we have a process for incident response. It is in place. Now what we don't have is a thick document explaining all this. But we absolutely have a responsive capability to work incidents.

In fact, Adair Martinez is in charge of that. She actually started it herself, organized the teams that meet weekly. She personally approves the weekly summary that is sent to Congress. Incidents do come in. They come into our NSOC, our network and security operations center. It is to the point now where this is routine, a routine process.

The one additional thing that we have to do is make sure we are folding in non-security incidents. And we are beginning to do that.

On security management, handbook 6500. It was signed out about a week ago. This is the security program for the VA. And, you know, I don't know if your Committee has had an opportunity to look at it yet or even if we have sent you a copy. But we certainly will. But this is now in place. You know, sir, it has taken—do you know how many years the VA's been working on this thing? How about ten. We have been trying to get this handbook called "6500" out the door for a long, long time. We have it. It has rules of behavior in it.

In fact, I have already met with the unions on this rules of behavior issue. These are very important for employees to sign. So the security management process is beginning to happen.

The other one that I would like to mention is the compliance management. And, again, we don't necessarily have one book that says compliance management. But in a minute I am going to ask Arnaldo Claudio to explain the process he has put in place, because it is very robust. It is very effective. And it is making a difference. It is in compliance.

The IT strategy, you know, we have completed a draft of our IT strategy. It is within several weeks of being approved. The other one I would like to mention is IT management. Some discussion took place about the governance structure. There is a governance structure in place.

The GAO report, unfortunately it was written at a time where we had not implemented that. We have. Those meetings have taken place in developing the FY09 budget in fact. We have had a number of meetings with all three of the governance boards that we have put in place, to include the IT leadership board, which I chair along with the Under Secretaries.

And so I wanted to just—sir, I wanted to paint a picture that, you know, we are really not sleeping. I mean, we are doing work. We are not there yet. I agree with you. But there is a lot of activity going on.

And one more thing I would like to say, sir, and that is it goes back to the problems that I mentioned. I am trying to maintain some balance. You know, I can beat the heck out of these people and make them focus on processes solely. Or I can try to balance their workload and make them solve these problems. And at the same time, put the processes in place.

And that is kind of what we have to do. And, unfortunately, it has resulted in a bit of a delay on some of these processes. But, again, some of them are already in place.

[The prepared statements of General Howard and Mr. Claudio appear on p. 71 and p. 72.]

The CHAIRMAN. Mr. Bilbray had mentioned earlier, and I always can't vouch for his accuracy, but he said it is easy to put biometrics on a laptop. Is that in your book there? Is he right? And do we——

General HOWARD. Sir, we——

The CHAIRMAN [continuing]. Have it in a book?

General HOWARD. We have looked—we have looked very hard at biometrics. And I can tell you that one of the concerns actually comes from the medical community, because sometimes these are not perfect. You know, they are not as foolproof as you might think. You know, it is pretty close, but it is not 100 percent.

We have looked at biometrics. The—it will not work as smoothly as you would like with the encryption application that we have placed on our laptops. We have Guardian Edge hard drive encryption. If a VA laptop is left out on the parking lot, it is useless. It has got full hard drive encryption on it. It is useless to anybody. You can't get in. You simply can't get in.

So that part of it is very robust on the laptop side. We do have biometric thumb drives. In fact, I have one in my briefcase. You know, we have mandated the use of encrypted thumb drives across the VA. And one of them happens to be an encrypted version. I mean, a biometric version that can be used.

So we have—we have employed that to some degree. In the—and while I am on this issue of protecting the information or what have you, we have had a number of initiatives underway. And have worked very hard during this fiscal year to put contracts in place for the software as well as the implementation of that software, the rollout. I am going to mention a few.

We have put monitoring software now. And I think at an earlier meeting I may have mentioned the importance of that. I know I did to Jeff and Art. This Port Monitoring software, the contract was put in place about a week ago. We are not rolling that out.

That means whatever you stick in a port on a VA laptop, we are going to know what it is. And we are going to stop the use of it if you don't have a VA approved encrypted thumb drive, for example, you can't use it on a—in a VA computer.

Now, obviously, it is going to take time to roll that out. We have enough licenses to cover all of the VA in that particular one. Another one is called Rescue, the remove enterprise security compliance update environment. This one, if you are sitting in your kitchen somewhere, you will not be able to download personally identifiable information. We will stop that. You can see it if you have authority through a secure tunnel, through a virtual private network (VPN) tunnel, you will be able to see the information and do your work. But you won't be able to download it, because we will stop it with this particular product.

We are monitoring the network for Social Security numbers. You know, you read the reports that we send up here every week. And you can see that unencrypted emails have been a problem, you know, sending Social Security numbers in the clear.

We are monitoring that now. In fact when we first started monitoring it, there were almost 7,000 incidents of likely Social Security numbers, you know, trafficking through the network. We put a warning sign on the computers. You know, boom, it will come up as soon as you try to do that. Give you a warning.

And since that time, it has gone down. We are now blocking those messages. We have gradually moved to the point where if you try to send a Social Security number in an email it will be blocked. On email encryption, you know, right now in the VA to include Blackberries, we have PKI, public key infrastructure.

It is very good. But it is not as robust as the product that we are now implementing. In fact, IBM just won the contract, I believe, Charlie, right?

Mr. DE SANNO. That is correct.

General HOWARD. For RMS, Rights Management System?

Mr. DE SANNO. Yes.

General HOWARD. That is a product that will—you can send an email in the clear. But the attachment is encrypted. It gives you a much better—much more flexible capability to work encrypted email in a variety of ways, a very important one.

We have software in place now for port-to-port transmission. You know, the VistA system when it was developed, did not take security into consideration as much as we would have today. So we now have in place a host-to-host secure capability that we have been working on as well. And the final one that I would like to mention in this whole area of trying to protect information and be more standard about that is the Dell Computer contract that we just put in place. And you are aware of that, standardized desktops. The Office of Management and Budget (OMB) has mandated that desktops will be standardized throughout the government agencies.

This will provide a much better capability. It is a lease contract. We will every two or three years refresh the equipment. And we will be able to monitor it much better. We will be able to put whatever we want on it. The people who are working the computer will have much less control over what they do.

This will be enormously helpful to us, not only in terms of standardizing things, but helping us with this issue of security. It will be very helpful. And, in fact, Charlie just this morning showed me the sites that we are likely to start rolling this out beginning this particular fiscal year.

And there are other activities. The one I would like to mention also has to do with training and educating the people, because as we have mentioned in this Committee before, sir, I know the Secretary has, you know, the real key here no matter all this—all these tools that we put in place, the bottom line is are the people paying attention? Are they using the tools the right way? Are they properly educated? Do they care?

We have seen improvement in that area. We do have a way to go. Education programs are better now. They are in place. We—I strongly believe that our directors throughout the VA are serious about educating and training their people.

And that is a very key aspect, not just the IT people; it is everybody who deals with, you know, personally identifiable information. And quite frankly, that is very extensive throughout the VA as you

can certainly appreciate. I don't know if that is helpful, sir. But there is a lot going on. And sometimes you don't get the complete picture.

The CHAIRMAN. I appreciate that. You identified Mr. De Sanno as head of region four.

Mr. DE SANNO. Northeast, sir.

The CHAIRMAN. Region—what region four?

Mr. DE SANNO. Sir, the——

The CHAIRMAN. I mean, not the Veterans Integrated Services Network (VISN) four?

Mr. DE SANNO. No. The regions are numbered from the West Coast to the East Coast. So region four is comprised of VISNs one through five and VA's central office.

General HOWARD. What Charlie is describing, sir, is the way we have organized the information technology——

The CHAIRMAN. So we have regions to coordinate the regional coordinators.

Mr. DE SANNO. Well, yes. We have—well, you know, in an immense healthcare system like the VA, we segment the business into various management structures. So we have a regional director and chief technology officer responsible for the regional activity.

General HOWARD. Sir, the reason we have done that refers to span and control. When we took over all 6,000 people, the way the VISNs are, you know, they are throughout the country and they are not regionalized. That is much too big a span and control in my opinion.

So we put down four regions. There are regional directors in charge of each one. CIOs at a facility level report to that regional director. I meet with them quite often. The four regional directors report to my Deputy Assistant Secretary for Operations.

That is how it works. And, in fact, it is a pretty good control structure. Communication is very good in that structure. The communication problem we see is with our customers. You know, that is the part we need to work on better.

But within the IT community, we have visibility about what is going on. And I broke the region—the country into those regions simply as a matter of better span and control.

The CHAIRMAN. Okay. Let's look at the three measurements that were mentioned in the earlier testimony.

We had 17 recommendations by the IG. We have 36 management processes that you were working on. We had 25 key positions of which, again, the report that we heard, 15 out of those are vacant.

Only two of the management processes have been fulfilled in one of the seventeen recommendations. So what is your timeline for completing that process?

General HOWARD. Sir, the——

The CHAIRMAN. When are you going to fill these positions? When are you——

General HOWARD. Sir, quite honestly, I am not sure what positions they are referring to. I do know some that are empty. But I don't have the list in front of me, all 15. The—one of the issues there has to do with the human resources (HR) process itself.

The CHAIRMAN. Yeah, that bothers me. Is the GAO still here? Is Ms. Melvin still here? The report states there are—that there are

25 recognized—that you identified 25 key positions for carrying out these processes, and about 15 of them were vacant. And you are not even sure which ones she is talking about.

General HOWARD. Sir——

The CHAIRMAN. So there is a problem there. I mean——

General HOWARD. Sir, I don't. I can't get to the number 25. What I would like to do, if it is okay with you, sir, is answer for the record.

You know, we can get from GAO exactly those positions and tell you——

The CHAIRMAN. Okay. But as I understood it, and my understanding may have been wrong, but as I read the report, you identified these 25 positions. The GAO didn't make them up. They came from you. And so I assume you are aware of your organization and how we got to that figure.

General HOWARD. Sir, as I sit here today, it is not 25.

The CHAIRMAN. What is it?

General HOWARD. Sir, I would like to answer that for the record, sir.

[The information was provided from General Howard is in the response to Question 1 in the post-hearing questions for the record, which appears on p. 82.]

The CHAIRMAN. Right.

General HOWARD. Because I want to match it exactly to what appeared in the GAO report, if that is okay with you.

The CHAIRMAN. Okay. Sir, I asked about a timeline on——

General HOWARD. And you mentioned—you mentioned what difficulties we are having with respect to hiring. Part of it is just the HR process itself. This is very time consuming.

An earlier Member mentioned, you know, the ease with which IBM or Microsoft could deal with this. And he is exactly right. We are not a private company. I came from a private sector. And we can hire and fire at lightning speed in comparison to the way we have to work in the government, particularly for senior positions.

For example, one position that we have been struggling with is a very, very important one. It is cyber security. We have been through iterations. Three lists of people in the last—the last list we had actually selected someone. And they declined at the last minute to come in.

We now have the latest list. And we are within weeks of making a selection. We got a much—we went out further, expanded our search, and we have a much better list. So you asked about why are we so slow, that is one of the reasons. It simply takes time to hire people in the U.S. Government.

Sir, the timeline for filling positions, again, I would like to look at the detail there and respond for the record, because I need to be accurate in what I tell you. Because I need to see where we are on the hiring of some of these.

[The information on timelines for filling positions was provided from General Howard is in the response to Question 1 in the post-hearing questions for the record, which appears on p. 82.]

General HOWARD. I mentioned cyber security. We were pretty close on that. The timeline on that one, for example, is a couple of weeks. You know, maybe 4 weeks at the max. We will have a

name. And then it has got to work—it has got to work through the process, because this is a senior position. And it has got to work through, you know, our senior leadership and Office of Management and Budget and the Office of Personnel Management (OPM).

The CHAIRMAN. Well, how about these 36 management processes? The——

General HOWARD. Sir, I am committed to have implemented these by the summer of 2008. You know, that is the—July of 2008 is when we—is when we complete our reorganization. And that is what I am committed to implementing.

A number of them have already been implemented. We just need to capture in written form what we are actually doing, the incident response one is a good example. But that is what I am on the hook for.

[The additional information was provided from General Howard is in the response to Question 2 in the post-hearing questions for the record, which appears on p. 85.]

The CHAIRMAN. Okay. Just for the record, this is from the GAO testimony on page 15: "As part of the new organizational structure the Department identified 25 offices whose leaders will report to the five deputy assistant secretaries, and are responsible for carrying out the new management processes and daily operations. However, as of early September, seven of the leadership positions for these 25 offices were vacant, and four were filled in an acting capacity."

So I assume we know what positions we are talking about.

General HOWARD. Yes, sir. And some of them, as I said, was an acting capacity. And that is why I wouldn't consider those as being unfilled.

For example, my position for Enterprise Strategy Policy Plans and Programs is filled right now in a temporary way by Scott Craig. He is a very strong person. He has been my enterprise architecture guy for years in the VA. So it isn't like the position is empty. I do have—I do have someone in there.

The CHAIRMAN. You just don't do the same thing as an acting as compared to a permanent employee. We had this crisis situation now 16 months ago. And, I mean, if I were the Secretary, if I were you, I would have been calling us up and saying, we've done this or we've done that. It has been only 5 months since this loss. And we have all the computers encrypted; it is now 8 months and we have this reorganization. It is now 10 months and so on.

We don't hear from you until we call you. It is as if you say, well, no way around it, I guess we have to tell these guys now how many positions we filled. And everything just goes on as if it is a normal situation. That's what it looks like to me.

There is not a sense of urgency that we had last year. And the fear that was so rampant throughout the veterans' community that their personal data may have been stolen or their identity may have been compromised was palpable. We simply must have a fast response on this stuff.

If there are things that are getting in the way of doing that, just tell us and we will try to make it easier. We are working together on this; it is not just grilling you every 3 months about what is happening. We want to help you accomplish this.

Mr. Bilbray.

Mr. BILBRAY. Thank you, Mr. Chairman. Mr. Howard, I was sitting here just—and I made a flippant remark to the Chairman about the days when we were in local government. But I just realized there was a reason why.

When we were looking at IT and upgrading systems, we finally abandoned doing it in house. And started putting it out for bids for private companies to come in and competitively bid, because there was a degree of urgency then.

And I guess the Chairman's concern is the fact that, yeah, these things go on and nobody is accountable. Also no one is fired. Except maybe you want to get rid of the guy at the top. But we all know mid-management is where these things are really done.

I would just like to follow up, and I don't mean to ping on this thing, but you made a comment about the fact that medical—there were people in the medical field who were concerned about the biometric confirmation for access. Why would they be concerned about biometric confirmation for access?

Except maybe the fact is do they understand what we are talking about? It is access to the—into the computer, not necessarily access into the records?

General HOWARD. Sir, it is reliability issue. You know, in some cases it doesn't work right away. You may have to work your thumb a few more times. I mean, it is not as rapid. And in the medical community that is a concern.

Mr. BILBRAY. And the laptop—the laptop though, that is not where they are using it is it?

General HOWARD. Sir, I think you may be referring to the laptops associated with medical devices that are not encrypted. This is a problem for us. And the issue is this, a lot of your medical equipment these days does have integral to it a laptop or at least some kind of software. And these devices have to be approved through the Food Drug Administration.

You have to be very careful about what you put on that machine. In fact, you can't put some things on.

Mr. BILBRAY. Yeah. I understand that. Let me stop you and back up a little bit. We just made a huge leap from the medical—basically the veterans' records, not—but the veterans' records on laptops that are being carried, being taken home, are being carried on airplanes, are being stolen.

That is a huge leap to go from the equipment at a medical facility and the access into that system. I just go back to the fact that we have so many of these laptops out there. We don't even know how many we have now, because you got——

General HOWARD. There are 18,000——

Mr. BILBRAY. Eighteen thousand——

General HOWARD [continuing]. VA laptops.

Mr. BILBRAY [continuing]. VA. How many private laptops that have VA access?

General HOWARD. Sir, I don't know the answer to that.

Mr. BILBRAY. Yeah. And I think we agreed that needs——

General HOWARD. It is vulnerable. Yes, sir. However, I will say this, there is a directive. In fact, I believe it is 06–5 or something. I can't remember the number. Where—this is the waiver issue.

That in order for the physicians to continue to do their work, we did put a waiver in place with the proviso, with the directive, that they have to protect their laptop in the same manner that the VA has.

In other words, we have Guardian Edge full drive—full hard drive encryption on VA laptops. If you are a physician in the VA using your own personal laptop, you have to have equivalent hard drive encryption on your laptop. That is a mandate.

Let me say one more thing, sir, one of the technical items that I mentioned earlier will be helpful to us to prevent you from downloading anything on your laptop. And that is being put in place right now. You know, that was a very important contract that we have been working on for months. We now have it.

We will have help from the private sector. In fact, we have help from the private sector at all of these areas. But that will not only—not only protect the information. You won't be able to put it on your laptop, because we will not allow it. And that will be very helpful to us.

Mr. BILBRAY. Okay. Mr. Howard, you know, the Chairman was questioning why—you know, about this issue of the biometrics. And the way I ran into it, because I have a district with a lot of high-tech biotech people that want privacy for their information, need security. And they use this as a matter of fact.

And all my point was is that the security of the information of a company working on a new substitute for whole blood or doing something on cancer research, that information being secure is no more important than the right of a veteran to have their personal information secure.

And that is why I brought up this issue of if the private sector can do it, if the laptop computer companies are making this technology available as an option, it just seems like common sense that if we want to talk about truly securing, then we don't ever depend on one gatekeeper.

I mean, those of us that build jails know that you always have multiple catch systems so that when they are going through one, the other one will catch them down the line.

And I just ask us, again, the technology is out there. The private sector has been doing it. It is available on the general market. It is not rocket science. And we still are finding arguments to not use technology that the private sector has found very effective out there.

And I just ask us to, again, not to be scared of technology, but to embrace it. Not to put out the fire, because it may burn somebody. But realize that without it, a whole lot of people are going to go cold. I just think that we need to tool up on that.

And I just leave you, again with the argument that maybe the problem is, is that we have a system where you can't go in and fire people who are not performing and making sure that you can come to us with a more effective report.

General HOWARD. Yes, sir. Sir, I don't agree—disagree with you on the technical issue. I really don't. And as I mentioned, we are using biometric in the—particularly in the thumb drive area.

I would ask—in fact, Charlie De Sanno, in addition to directing region four, he is my systems engineer. All this technical stuff that

we are testing and rolling out and all that, a lot of that has come out of region four. And I would just like—if it would be okay, sir, for Charlie to just elaborate a bit on that.

In fact, right behind him is Jim Breeling. Jim is also up in region four. He is actually a physician. And between the two of them, they can elaborate quite a bit on some good things that are going on.

Go ahead, Charlie.

Mr. DE SANNO. Thank you, Mr. Howard. Excuse me. I think prior Mr. Howard gave you a good run down as to the products that the organization has procured.

And I think the point certainly needs to be made that with the reorganization of IT within the VA, certainly the infrastructure that Mr. Howard discusses, the haves and the have-nots, come into play significantly in a number of ways.

So we talk about speed to market. We talk about how quickly the VA can react to your requirements, to the veterans' requirements. And all of that is extremely valid point.

The problem that we have in the organization is that we first need to create a foundation to create our house. And it took some time to execute, to design that foundation. So when you look at any one technology, like biometrics, and you say hey, why isn't the VA using biometrics?

Well, we have a strategy behind everything we do. What you are really talking about is dual factor authentication and securing of the personal information that may exist on that hard drive.

The Personal Identity Verification (PIV) initiative with smart cards is going to be rolled out. And our architecture, given the mandate to use these smart cards, do work very nicely with our encryption.

Furthermore, with the PC lease and the standard desktop, the secure desktop image that we are "architecting" that is in line with standards, government-wide standards for security, we don't store any data on these mobile devices. The mobile devices and desktops and laptops, those data will be stored in a secure data center that is backed up.

And in addition, Mr. Howard references rescue. And with this product, we can ensure that the devices that are attaching to the VA network are not only secure but contain no data.

And if those devices aren't secure, we put them through a white room, a clean room, where we ensure that the Microsoft patches are up to date, other virus vulnerabilities are remediated.

And if we can't do it, ensuring we give that user a quick response time, we segment them. And we put them in a virtual environment.

So I agree as Mr. Howard does overall with the strategy. I want you to know that we have thought out this process. And we know that protecting veterans' information is absolutely critical.

There is a strategy behind what we are doing. And the foundation that we are putting in will be used to build all information technology for now and in the future years.

General HOWARD. Sir, this fiscal year is a key year for us. FY—you know, you asked about timelines. FY08, in fact the GAO mentioned this plan we have with 400 actions and all that.

You know, your guys have copies of that. FY 2008, although some of the timelines go beyond—our 2008 really is a key year. It really is.

And we expect to see very dramatic improvements in this whole area, because we got the tools in place now to help enforce some of this stuff that we did not have before.

Mr. BILBRAY. Do you have the money to pull this off though. I worry about the fact that I have seen again and again where we have done this. We have the mainframe set up, we get it all lined up, and then it doesn't connect. And we end up like the IRS did with a billion dollar system that doesn't work.

General HOWARD. Sir, we do—we do have the money, unless somebody takes it away from me, which they haven't yet. I mean, I feel reasonably comfortable. We are okay there.

The CHAIRMAN. Thank you, Mr. Bilbray. We thank you all for being here. As you heard, we have another set of votes. We are going to recess for 15 minutes. And then we will hear from the next panel.

Please understand our sense of frustration. We want it yesterday. None of us underestimates the difficulty. But without goals, without timelines, by pointing to the next fiscal year, it is always a process and it never gets done. And we want it done. If you need more resources to do it, you need to ask us.

Thank you again for being here. And we will start with panel 3 in about 15 minutes.

General HOWARD. Thank you, sir.

[Recess.]

The CHAIRMAN. I apologize for having to hold you all morning. I appreciate your being here. The third panel is comprised of Dr. Paul Tibbits, Deputy Chief Information Officer, Office of Enterprise Development, U.S. Department of Affairs. And Doctor Ben Davoren, Director of Clinical Informatics. Is that right? Is that a new word? You'll have to define it for me. At the San Francisco VA Medical Center. Please, I appreciate you staying through the afternoon here.

STATEMENTS OF PAUL A. TIBBITS, M.D., DEPUTY CHIEF INFORMATION OFFICER, OFFICE OF ENTERPRISE DEVELOPMENT, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND J. BEN DAVOREN, M.D., PH.D., DIRECTOR OF CLINICAL INFORMATICS, SAN FRANCISCO VETERANS AFFAIRS MEDICAL CENTER, VETERANS HEALTH ADMINISTRATION, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF PAUL TIBBITS, M.D.

Dr. TIBBITS. Thank you so much for the opportunity to testify in the realignment process in the Office of Information and Technology (OI&T) and to share with you the progress made in VA as a result of the centralization of development activities.

Joining me on this panel is Dr. Ben Davoren, Director of Clinical Informatics in San Francisco and Dr. Jim Brieling. You have just heard testimony from Assistant Secretary Howard regarding our

realignment progress and the need for more work to transition from a decentralized to a centralized organization.

I would like to share with you our progress establishing an IT governance plan, strengthening development processes—development process improvement efforts, and fostering innovation.

You have heard also General Howard refer to his seven priorities or you would have had he used his prepared remarks. But in any case, I would like to discuss with you those that directly apply to us in development.

First with respect to establishing a well-led, high-performing IT organization, we are pursing improvement of the development of workforce throughout the Office of Enterprise Development.

To improve the VA IT development workforce, we are instituting real-time coaching and mentoring by industry experts in best practices in systems development to institutionalize these practices in the VA.

Second, standardizing IT infrastructure and IT business processes throughout the VA provides a baseline for measuring effectiveness of our development process. It is the first step to reduce time to deliver applications, reduce costs to develop applications, implement process performance measures, and increase productivity of the development of workforce. And it is certainly very hard work.

We are using independent industry consultants to guide us through this self-improvement initiative.

Third, let me address establishing programs that make VA's IT system more interoperable and compatible. Interoperability begins with a common understanding of terminology.

The IT development organization will be collaborating more closely with the Administrations in the use of business modeling to perform—I'm sorry, to provide a uniform basis of developing a shared understanding of new ways to serve veterans and the information required to do so.

We are engaging with the administrations and with DoD to strengthen and accelerate data standardization activities within VA and with DoD. We are exploring ways to focus on high priority patient groups, such as traumatic brain injury and post traumatic stress disorder, while continuing the hard work of semantic analysis, reconciliation, and the consolidation of multiple data feeds between VA and DoD. Fourth, we are focused on managing the VA IT appropriation to ensure sustainment and modernization of our IT infrastructure and more focused application development to meet the requirements of our business units.

We are applying life cycle and total cost of ownership management practices to all development projects, to account for all costs of implementation and operations, as a foundation for budget formulation.

We are moving toward clear line-of-sight alignment with the VA strategic plan and the Performance Accountability Report by reshaping OMB 300 exhibits in fiscal year 2010, a creation of the first multi-year IT budget in VA, and strengthening our relationship with the requirements processes of the Administrations and staff offices.

With respect to governance, we have established a participative transparent IT governance process at the senior executive level of the VA. We have created a set of organizational principles and governance structures and practices that surface business strategy; facilitate accurate project cost, benefit, and risk estimation, and provided the decision-making framework that focuses attention on the most critical projects. We are developing management dashboards to implement early warnings of issues with system development.

The single IT appropriation sets a context for competition among new ideas, since some are not affordable. This creates the perception at the hospital level that many good ideas are disregarded despite "local needs," and that the flexibility available to VISN and hospital directors to use healthcare funds for information technology is constrained.

This disregards the rest of the story. Solutions developed locally, with a few exceptions, were rarely deployed across all VA medical centers, resulting in some centers not getting the advantage of these IT capabilities.

Furthermore, many needs were thought of as local, when in fact they were enterprise-wide requirements. Under the single IT authority and single appropriation, IT appropriation, we operate in an environment of financial transparency. Funds dedicated to sustainment, extending legacy systems to meet urgent needs of returning warriors, and to modernize our computing environment are now visible to senior VA executives.

Unmanaged local innovation makes the implementation of enterprise solutions quite difficult. Many IT products are operating in various VA medical centers, with no support mechanism to proliferate the more successful of them to all other medical centers.

In close collaboration with VHA, we are moving to create a process to identify new ideas at the local level, facilitate collaboration among field developers and VA medical center healthcare professionals, and to develop new software products in a non-production environment in an unconstrained manner.

In order to enter the live production environment and assure deployability across VA, certain technical assessments, business values, security, and patient safety assessments will be made and any remediation necessary applied.

The migration from the VistA legacy system to the HealtheVet platform entails complex development. This form of innovation must be centrally managed. It is too large for local initiatives alone to accomplish.

In addition, some forms of new IT support require an analysis of end-to-end processes to serve veterans, such as transition from DoD to VA, again not necessarily—not easily accomplished at the local level given complex data standardization and security issues that are involved. We are attempting to strike the right balance.

We have had some problems. But we have also gained valuable visibility over unknown IT—heretofore unknown IT activities, a definite improvement.

We also now know more about IT funding details across the VA and have a greater ability to protect sensitive veterans' information.

In closing, let me say that we want your ideas. I want to assure you, Mr. Chairman, that a successful IT realignment activity is a key goal within the VA.

We have accomplished many things this past year but much more remains to be done. I appreciate having this opportunity to discuss this with you and will gladly respond to your questions.

[The prepared statement of Dr. Tibbits appears on p. 73.]

STATEMENT OF J. BEN DAVOREN, M.D., PH.D.

Dr. DAVOREN. Medical informatics or clinical informatics is the science of information management, including all of terminology as well as human computer interfaces and so forth. So it is actually quite broad. It is not yet a medical specialty but it is being considered for one as we speak.

Good afternoon, Mr. Chairman, and Members of the Committee. I do want to thank you for this opportunity to provide my personal perspective of the OIT reorganization that began in 2005. But the views that I present today are my own and do not necessarily represent the views of the VHA.

By way of training, I am an oncologist. But I have been a member of the clinical work group that has helped guide the computerized patient record system development in VHA since 1999.

In response to the Secretaries proposal for IT realignment, many employees at medical centers expressed concerns about the details of the plan. And in particular, they felt that the regionalization of IT resources would create new points of failure that could not be controlled by the sites experiencing the impact of those. And that system redundancy required to prevent this was never listed as a prerequisite to centralization of critical patient care IT resources.

From my point of view, it was clear to me that the focus of reorganization was on technical relationships and not on how the missions of VHA could be communicated to the new OIT structure. And I communicated this to my facility director and VISN director at that time.

The IT reorganization has had a direct impact on VHA's four principal missions: patient care, education, research, and supporting the Department of Defense.

With respect to the primary patient care mission, the good news has been that new policies and procedures, in particular regarding encryption of sensitive information, have been very well-publicized and have heightened the awareness of all care providers as to the critical nature of the information that they, that we, use everyday.

The bad news is that centralization of physical IT resources to the regional data processing centers has directly led to more system downtime for individual medical centers than they have ever had before, resulting in hundreds of simultaneous threats to the safety of our veteran patients.

Disagreements about whether new clinical application requests are IT or not-IT has delayed implementations. With respect to the education mission, the good news, again, is that awareness has been heightened for staff and students about the information that we use and the need to protect it in all settings.

However, rules on encryption of all portable devices, such as thumb drives, rather than just on encrypting sensitive information,

have made it cumbersome to go about common work, such as giving academic talks where no scientific information is present. And collaboration by video conferencing has been curtailed.

With respect to the research mission, plan standardization of VHA databases may well and should create significant and very welcomed research opportunities. Though at this time, I don't have any specific progress to be able to report.

In terms of our role in supporting the Department of Defense, I believe that initiatives to enhance electronic data-sharing between VHA and DoD have proceeded appropriately from the field perspective.

But in my opinion, there has been a lack of transparent communication between VHA and the reorganizing OIT structure. At present, economies of scale that were a cornerstone of the realignment proposal have not been communicated to the facility level where the work of VHA occurs.

The focus on security and data integrity has led to a number of new requirements with impacts that generate significant concern without a clear pathway to resolution. In my view, there also remains a tremendous uncertainty about how to work with our longstanding IT colleagues to address local or regional clinical care, research, or educational needs.

These arise on an almost daily basis as the result of new mandates from accrediting bodies, VA performance measures internally, or Congressional action.

A word about the down time on August 31st. The new region one of OIT-supported facilities experienced the most significant technological threat to patient safety VA ever had. A 9-hour downtime during standard business hours that crippled the clinical and other information systems of 17 different VHA medical facilities.

During the downtime, it became clear that many assumptions about the Regional Data Processing Center model were erroneous.

Specifically, rather than creating a redundancy to protect facilities from system problems, a new single point of failure caused a problem that could never have been replicated without this Regional Data Processing Center model having been created.

In my view, the OIT realignment process begun in 2005 for the right reasons has been focused on technical IT issues and the reporting structure of its new 6,000-strong employee force and not on linking IT strategic planning with organizational strategic planning.

Mr. Chairman this concludes my statement. And I will be pleased to answer any questions you may have.

[The prepared statement of Dr. Davoren appears on p. 76.]

The CHAIRMAN. I didn't notice a lot of publicity about this downtime incident.

Dr. DAVOREN. On August 31st?

The CHAIRMAN. I don't remember it. The press didn't cover this, did they? Why do you think that was?

Dr. DAVOREN. It consumed our day, but I am unclear on what the press did or did not cover.

The CHAIRMAN. I mean you call it the most significant technological threat to patient safety the VA has ever had. You would

think somebody would have made a—I think we would have had a Congressional hearing on it actually.

So you are saying that the path that the VA took in terms of two different streams was very useful in that situation. Is that what you were saying? Phrase it for a layman so I can understand it.

Dr. DAVOREN. I am not sure I understand the question completely.

The CHAIRMAN. You said that we caused—I assume because of the centralized nature, a failure led to a very——

Dr. DAVOREN. That's right.

The CHAIRMAN [continuing]. Deep problem. And then you said—I see. I misunderstood what you said. "A problem that could never have been replicated."

Dr. DAVOREN. Right.

The CHAIRMAN. I don't know what that means.

Dr. DAVOREN. In other words, before the regionalization of IT resources with individual—the actual systems that contain the patient information in a distributed fashion at the medical centers, it would have been impossible to have 17 medical centers simultaneously have their clinical information systems unavailable. But that was the case.

The CHAIRMAN. Okay. So you are saying the centralization has ended up with this downside.

Dr. DAVOREN. The—yeah. Centralization of the physical IT resources.

The CHAIRMAN. Okay. That was the theme of your statement that the local kinds of needs may be either overlooked or washed out in terms of this.

Dr. DAVOREN. That there isn't a clear pathway of communication. And——

The CHAIRMAN. How would you remedy that?

Dr. DAVOREN. Well, I think—I think there are a few key areas. From the facility level, the changes that have occurred in terms of our collaboration with our IT colleagues, it is not clear exactly what we can and can't do when we approach problem solving at the medical center.

We have a number of—we have a number of internal and external bodies that tell us that things need to change as medical care evolves. And many of the processes that we have involve an IT component.

So if we have a new discharge process for example, because we know our hospitals are very, very full, there may be some human resources as a project—a process action team, as we call them, typically looks at the causes of a problem. And looks for areas where we might be able to solve them.

So a very, very full hospital trying to improve the discharge process is a key item. We may find that we actually need to hire a discharge planning nurse or a pharmacist. We may need to set aside some physical space. And we may need to make some changes or we would like to make some changes to how the computer system works, generates output for some of these people at the time of discharge.

In the past, that was—we had a team. They all worked for the medical center. And so this whole process would be put together.

Now that team, on paper for sure, no longer exists. So the question is at this point, for our region in particular, if we can't make local changes to our internal VistA system, it is not clear what the communication method is back to the resources that now live in OIT to accomplish that.

The CHAIRMAN. What did you call—you had some coordinator of beds. You had a title to help——

Dr. DAVOREN. For the discharge planning?

The CHAIRMAN. Yes. What was the title?

Dr. DAVOREN. So a number of VAs have looked at this process because it is so critical. So there are discharge planners——

The CHAIRMAN. Discharge planners.

Dr. DAVOREN [continuing]. Who are frequently——

The CHAIRMAN. You should call them "ombudsmen."

Dr. DAVOREN. I will make a note of this.

The CHAIRMAN. The only guy who laughed was the guy I pay. I am told by the counsel that you have used the chemotherapy software as a good example to highlight some of this. Tell us about this.

Dr. DAVOREN. Right. As a highlight of where the communications process is very unclear, it—there is a product that happens to be called IntelliDose. I am an oncologist, so I do write for chemotherapy.

And this is a particular software that integrates with the VistA system, with the core VA system, for writing chemotherapy that the existing VistA system cannot do. And that immediately planned VistA systems will not do.

So there is a system that has been piloted at the San Diego VA and integrated with VistA over the last couple of years to really work the bugs out in a real-life setting.

And the—in the VHA structure, the Impaired Decision Making Capacity (IDMC) that was referred to earlier this morning, would—did make a decision about a year ago that it was ready for prime time if you will. The software was mature enough in its integration that it could be used at other medical centers besides the pilot site.

We wrote a proposal after reviewing the software for my network, VISN 21. We got the clinical buy in. We saw a number of demonstrations to be sure this is what we wanted to do. And I wrote a proposal for the project.

It was, by my own interpretation of the rules of what is or is not IT, really more of a medical device and not an IT expenditure. But that was not agreed with by the VISN CIO necessarily. And that as we wrote the proposal and were able to get funding, then suddenly a few weeks ago it was determined that this really ought to go back to the IDMC for not just their review and approval, but for review and approval for national funding.

And the Western States Network Consortium that was—in region one, so the West Coast networks decided that perhaps this might be one of the pilot projects they would like to do at a regional level. So the particular proposal that I put together was on hold.

So what this has the effect of saying is that we had a community sense of what needed to be done. We had a pilot project that proved—that proof of concept. We were ready to go forward for

FY08. But now there is a new layer of review that is not entirely clear to me what exactly it is that makes this looks like it may not be—until 2009 or 2010.

So it is going back to the IDMC body that originally says it was okay to get with a new task for the IDMC. I recognize that is very circular. But I am just trying to convey the sense that from the field perspective, the communication about what really needs to be done to implement something that our patients need now is very, very unclear.

The CHAIRMAN. How long have you been with the VA?

Dr. DAVOREN. I have been with the VA for 12 years.

The CHAIRMAN. Do you feel secure in your job? I am about to do something that has not been done. So I want to make sure I get your——

Dr. DAVOREN. I have told people I will find out whether or not I am a political appointee at this very hearing. So—but generally yes I do.

The CHAIRMAN. I should do this. General Howard, can you just come back to the table for a second. I am not going to have an argument between you. But you have heard us yelling about centralization, right? And there have been qualms.

We went from a very decentralized system, which had problems. Now we are moving to a very centralized system. And we hear there are problems with this approach. This is not the first person to raise these concerns. How do we find the balance there?

General HOWARD. Yes, sir. Let me——

The CHAIRMAN. And without, you know, reacting to every scream, we do one thing, and then we have gone too far, and now we have a scream about going the other way. And, you know, it is not a helpful process.

General HOWARD. No, sir. But I would—I will say that there is a process in VHA for elevating requirements to the very senior level. I mean, there is. And, in fact, I have actually participated in meetings of the Committee that does that.

I can't recall the individual who chairs that Committee right now. But it used to be Dr. Bob Lynch. Lynch has since left the VA. But there is a new individual now. I can't recall his name.

But that body is in place. They had functions to prioritize, you know, whether an issue is a class three requirement that needs to be put in place or any requirement from within VHA. That is the Committee that decides how those items are prioritized.

However with that said, there still exists at the facility level the capability to try out ideas and that sort of thing. And in fact, I will ask Paul Tibbits to describe the process. He mentioned it in his testimony that we in VHA are putting in place to make sure innovation does occur and continues to occur at the facility level.

But at some point in time, you have to begin to gather that up and expand it throughout the VA or else——

The CHAIRMAN. No. I understand that. But as I heard Dr. Davoren say—I mean, we have added, for example years, to a potentially very helpful therapy to try to test it or use it.

And so are we adding this level of bureaucracy that will take—I mean, clearly you want something to spread good things quickly. But——

General HOWARD. Mm-hmm.

The CHAIRMAN [continuing]. You want to also balance that without having good things coming to the surface without a bureaucracy interfering.

General HOWARD. Yes, sir. There—from an OIT standpoint, there is no—there is no OIT layer between Dr. Davoren and Mike Cuspin. We are not in that. We are in our own layer. You know, we have our own reporting process. But any requirement within VHA does not have to go through OIT. It can go all the way up to the top.

Now at some point in time, obviously we are engaged in the examination of that issue to first of all see if it is possible, see if there is funding available, and what have you.

The visibility issues, though, is key. You mentioned, you know, the decentralized way of doing business in the past. If I was a hospital director, in the past and before the IT appropriation, I did what I needed to do, you know, out of the medical money available. If I needed to spend it on IT I did. I mean, it was actually, if you were a hospital director, was not a bad environment. It was pretty good.

The trouble is it was not very efficient. And the Congress actually got pretty upset with that kind of operation. And that is what we are trying to standardize. We are not—we are trying to standardize this. But at the same time, not kill innovation. We definitely do not want to do that.

We want to put a better process in place to control it a little bit more so that the good ideas do bubble to the top and get used throughout the VA. And the ones that maybe are not very good, are finally just cut off. I mean, that is kind of a research environment that has to be——

The CHAIRMAN. Well, but another way to ask about that balance, I mean, again, it was mentioned, this region one downtime——

General HOWARD. Mm-hmm.

The CHAIRMAN [continuing]. That we lost the whole region. I mean, is that an example of over-centralization or not?

General HOWARD. It is to prevent——

The CHAIRMAN. How are we going to prevent that from occurring again?

General HOWARD. Sir, actually the—it is the regional data processing program. And it actually existed before the IT central. It was the VHA initiative that goes back a number of years.

And the idea, the central idea, was to better protect the information, you know, in well-protected data centers, tier four data centers.

Obviously at this point in time, we are responsible for that program. You know, it came over to us. So everything that happened at Sacramento is on our watch. You know, we were responsible for that.

What we are discovering—and just to comment on that, clearly, you know, we put a team in to examine what happened. The fact is the tiger team is still at work to examine the details of all that. I have an independent review that is about to get underway, because there is more to this than meets the eye.

We are very concerned about in the design of the program, for whatever reason, the proper backup at facility level was not adequately considered. We can see that now.

In other words, some facilities had a better capability to read, not write, but read information on their backup system than other sites did. You know, why was that dichotomy there?

And maybe we skimped from a resource standpoint. But we have an effort underway now to examine not just Sacramento, but the whole program to see exactly what we are doing and build in a more robust backup capability at the facility level. We have that underway and include the other data centers as well, you know, the corporate data centers.

So we are stepping back to take a hard look at this program to see exactly what we are doing. Some aspects of it are good. The idea of protecting the information is very good.

But you can't permit—you know, permit a condition that allows a hospital to go down for 8 hours. That is ridiculous. We cannot allow that to happen. We understand that. And we are going to take steps to do it. It may involve more funding. And we just don't know that at this time.

The CHAIRMAN. Any more comments on this issue, Dr. Davoren.

Dr. DAVOREN. On the down time?

The CHAIRMAN. Or on any of the issues we just raised.

Dr. DAVOREN. Right. I think, you know, ultimately the—if the end user needs, my needs and those of the people that I work with to directly care for the veteran in front of them, are the driver for processes that happen to include IT as a part of them. That the structure needs to be in place and more transparent to those of us who are in the field for how we can—how we can relay our innovative ideas as well as our concerns about day-to-day operations through the whole structure, through both our own VHA structure as well as the communication points to OIT. And from the field from the farthest point on the West Coast represented here that that is not in place.

The CHAIRMAN. Okay. I hope we keep that in mind as we go through this process. And we should bring in more people from the field to give us their sense of what is going on.

So thank you for your candid comments.

I just—Dr. Tibbits, if I just—this thing about DoD and VA just flabbergasts me. You know, in concept, interoperability is easy. But we have been talking about it for probably a couple of decades. Why is it so difficult?

I mean, could a General Howard or a Bill Gates come in and just say do it? What is so difficult about just ordering these two systems to talk to one another? I see some people shaking their heads that it couldn't happen that way. But why is that so—what am I missing here as a layman?

Dr. TIBBITS. Thank you for the question. It is an excellent question. And there are several ways to answer the question. And let me step through them quickly. And then allow more time for discussion if you wish.

At the end of the day, the reason it is not so simple to just say go do it is the vocabulary problem. The vocabulary problem is an intense problem. If you can think of "Roget's Thesaurus" of the De-

partment of Defense. It has got its—it would have its own thesaurus. If you think of "Roget's Thesaurus" of the VA, it would have its own thesaurus.

And without putting those two things together, it is extremely difficult to get interoperability to happen in the way many people want it. So if you back down from that and start saying, all right, are there simplifying constructs that we can use? So without getting our thesaurus——

The CHAIRMAN. Can't you have the "Howard Thesaurus" and——

Dr. TIBBITS. The what?

The CHAIRMAN. "Howard Thesaurus."

General HOWARD. You wouldn't be able to understand it.

Dr. TIBBITS. Well, we could. But what that creates, unfortunately, is a third thesaurus. And while, yes, if in fact—in fact that is a strategy. And if we got all parties to agree to that third one and mapped the third one, that would actually be progress.

But I want to back down from that and say there are simplifying constructs. And those simplifying constructs involve not going for the full degree of information interoperability. So a computer can actually recognize the information. But simply transmit electronic information back and forth that the computer can't read, but a human being can. But it is still in the computer. All right?

So we have done that. We have gone down to a lesser degree of information interoperability. And there is a great deal of clinical information that is going back and forth and scheduled to be augmented over the next few months between the two departments.

And Mr. Bestor and Mr. Wu are very familiar with many of those initiatives, VA Health Information Exchange, Federal Health Information Exchange. Lots of information going back and forth there.

The other piece of it is organizational. And let me just touch on that.

The CHAIRMAN. I am sorry, go ahead.

Dr. TIBBITS. Let me just touch on that lightly. Organizational—I have personally been involved in looking at the organizational implications of what you are saying for many years, both when I was in DoD I spent a lot of time working on VA DoD collaboration. I had 26 years in the Navy Medical Department, 18 of which were on medical informatics I might add.

I spent a lot of time on VA DoD collaboration issues. After that, I supported the Presidential Task Force and looked at DoD collaboration and wrote the chapter actually on seamless transition.

One of the issues then we focused on, and we still focus on now, is there are two cabinet level agencies. And who exactly is it that is going to tell two cabinet-level agencies on a practical day-to-day basis to collaborate with each other?

And when we go up the executive branch, what do we find? We find OMB in the White House. We were never convinced that as a practical matter of getting two cabinet agencies to collaborate with each other, either OMB or the White House, were really very effective management tools in the sense that that actually has to be managed. At a policy level, they may be quite effective. But to really get that to happen, is very difficult circumstance.

So I guess thirdly I would say requirements are important. What are we trying to exchange information for? And there is two big buckets here that I want to put in front of you.

One is to better serve veterans. The other is to save money. It is very important to look at those two objectives separately and figure out which one or both or which is it we are after and in what degree of priority.

If our primary objective is to serve veterans' needs, a program structure would evolve from that and has evolved from that, which focuses on the data, the clinical data, what is in the record, how the veteran and how the servicemember was treated in exchanging that back and forth.

If one is interested in saving money, then a whole different paradigm has to be taken, which looks at software and software development. And are we developing software together, we, VA and DoD, that would save money, that would allow us to reuse the software perhaps between both departments.

But that in and of itself, would not standardize the data so that we could have the information and operability necessary to serve veterans' needs.

So being clear about those objectives between the two departments, addressing the issues of how we get two departments from an organization perspective to collaborate with each other, and then forcing attention and more and more attention on the terminology issues to get the two departments to speak the same languages, are basically the three levels of issues that are relevant to your question.

The CHAIRMAN. If we actually solved this thing, you wouldn't have a job anymore. That is the real problem here I think. Just kidding, sir.

Dr. TIBBITS. I would be glad to relinquish my job and solve that, because I have been after this issue and this job for too long. And I can't tell you how much I appreciate your question.

No, we are solving it.

The CHAIRMAN. Again, as a layman, I mean, you use "Thesaurus I." What is the plural of thesaurus, a thesauri? Thesauramatics is probably a specialty. There is probably a specialty in the study of a thesaurus. You had one and two. And you—I suggested a third. Why isn't "Thesaurus I" adopted?

Dr. TIBBITS. Well——

The CHAIRMAN. I am told VistA is the best system in the world. So why doesn't the DoD adopt VistA?

Dr. TIBBITS. That doesn't solve the terminology problem. That is why. And let me try to exemplify that for you in terms that perhaps all of you—everyone will be familiar with. And let me use email as an example.

I assume many of you in the room today are familiar with Microsoft Exchange and use Microsoft Exchange for email, Outlook, Microsoft Outlook. I assume many of you at one time may have been familiar or used Lotus Notes. Two very different programs. Two very different sets of software. But yet information can be exchanged between the two of them, because if both users speak English terminology, if both users use the same standard protocols for transmission, TCPIP (Transmission Control Protocol Internet

Protocol), a little techno babble, if both of those standards are in place, then information interoperability can happen very clearly with the software on both ends, sender and receiver being completely different.

If on the other hand, you use Microsoft Outlook, and you attempt to send email to a Frenchman who is also using Microsoft Outlook, identical code on both ends, identical software, the same computer system, if you will, on both end, sender and receiver. You even use the same protocol, so the message will get through.

If you speak only English, and the recipient speaks only French, there will be no information interoperability with identical code on both ends.

That is exactly the situation we have now. If you take VistA, and the reverse is also true if you take Alta, either way. If you take VistA and power shoot it in the Department of Defense today, either it will have to be repopulated, the files and tables, with the terminology of the Department of Defense in order for them to be able to use it. Or they will have to change their entire terminology libraries to be able to use it with our terminology in it, which would be a massive change in policy, how they manage people, how they manage their budgets, how they do assignments, how they send people to theater, how they order band-aids. All would have to change to the VA's terminology model.

The CHAIRMAN. Couldn't I send my English email through a translator?

Dr. TIBBITS. Yes. And that is the terminology mapping. And to build those—that is—that is the thesaurus work of putting the two thesaurus' together. And either——

The CHAIRMAN. But then the Frenchman would understand me, right?

Dr. TIBBITS. That is correct. But that is the hard work. And that is why it takes so long.

The CHAIRMAN. That is hard. Okay, it just sounds easy to me.

Dr. TIBBITS. Very hard. Very—those are very large data sets. Imagine every drug. That—when we standardized drugs, that is just one domain. When we standardize allergies, that is just one domain. When we standardize vital signs, that is just one domain. And that is what we are doing.

And by the way, at the end of the day, we may not have necessarily addressed the data for traumatic brain injury. Why not? Because if you were to ask me well what have you done by way of standardization for traumatic brain injury, my answer would be, well, we have standardized drugs, we have standardized allergies, and we have standardized vital signs for them. Okay, Doc, but can you send the electro encephalogram back and forth? Well the answer is no. We didn't quite get to the wave form domain yet.

So my answer is both. Continue with the hard work of the thesaurus work. Continue with that. Keep that going. While at the same time, we superimpose on it a problem-oriented approach.

Take the big problems first, traumatic brain injury, PTSD, amputation, and look at a combination of both structure and unstructured data so that we actually have information inoperability, some of which is computable, some of which is not computable. But a physician can still read and develop our data exchange

plans that way, so it is a combination of both as a simplifying and acceleration technique to address the key problems that are important to veterans today.

The CHAIRMAN. Thank you. That was very helpful. I appreciate it.

Mr. Wu, did you have a question? You may. Please.

Mr. WU. Chairman Filner, we appreciate the accommodation for counsel to ask several questions. I will defer the questions to General Howard, since we argue all the time. And we don't need to do that here.

A little history. I don't need to ask Dr. Tibbits any questions, because he and I argued about the incompatibility or compatibility of DoD and VA for the last 10 years. And I was asking the same questions you were asking him before.

But I will ask Dr. Davoren. I now know who I want to come to as a hematology oncologist if I become afflicted. And I appreciate that.

The CHAIRMAN. It is oncologomatics is what he is——

Mr. WU. But your testimony concerns us. And I think, Mr. Bestor, the staff director on the majority side, and I have had this conversation before. He says, "I have pride of authorship." Since we did the Omnibus Act that did the integration consolidation, and Mr. Buyer put 6 years into it.

It is not that I don't have an appreciation for what you are talking about, what you want to do on the software program for chemotherapy protocols and so forth. I would just ask you this, how many in the VA system of 152 hospitals that deal with oncology, that deal with chemotherapy protocols, whether they are in clinical trials, that there aren't hospitals that are using some software now similar to what was demoed successfully in San Diego, not saying which is best, and how are they in the queue?

What if you have five different systems out there doing the same thing? Should we have five systems? Should we have one?

Dr. DAVOREN. At this point, I can tell you that there aren't any other integrated software systems in the VA specifically for this application. That is for me, that is what makes it such a no-brainer.

I think the issue for the bake-off, if you will, of competing products is very important. I think there are many layers to this, however. Every—there is a saying that you have heard probably too many times in this room that when you have seen one VA, you have seen one VA.

And that software by itself, does—it can enforce a specific clinical business process. But typically it is invested in a particular way of doing business.

So, for example, if you look at the discharge process I talked about before, there are some places that may address this with some changes in physical space. There are places that may address this in changes of personnel and responsibilities, hiring nurses, hiring pharmacists, hiring a number of people.

And they may also feel that there is an IT component that needs to be modified in those. And that doesn't mean that the IT component that is developed there is actually applicable to the way that another VA does business with the same exact problem.

That doesn't mean it doesn't need to be addressed. But in way of answering your question, it is not clear at the—at the point of care for the veteran in front of you that it matters whether or not the exact tool that you use is the same in San Francisco as it is in Puget Sound, as it is in New Orleans.

Mr. WU. All right. I can appreciate that. On the down time, Chairman Filner, it was very disturbing to see a network of hospitals down or be without access to clinical information. I think that is profound.

But I would ask you this, and I was relieved when those regional process data process centers went into place. Chairman Filner, I will tell you that I was detailed to the special investigative Committee on Katrina. And that was a good news story for the VA, because out of Louisiana State University, out of Tulane, out of Baptist Hospital, out of Charity, every one of their medical records were destroyed when the flood came through. The VA was able to download their medical records, which were on servers in the sub-basement.

What is significant about that is that is where the sub-basement is located. The front step of the VA hospital is four feet below sea level. So I can't imagine how far down further the sub-basement was.

The point of the matter was they brought them, they downloaded the tapes, put them on a laundry truck, if I remember correctly, took them to the Superdome, and airlifted them out of there to Houston, where they were downloaded.

Houston could not use the tapes, because the VistA system was different. It was tweaked locally. I think it was about 3 to 4 days before they could bring it back up, plus they lost all their images, their radiographic images, the x-rays.

And at that time, the question we had on the special Committee was—and it was a good news story and a bad news story for the VA—what happened? Why wasn't all the VA data available, because what I didn't realize is that all the data at each hospital, San Francisco is yours, and resides in San Francisco.

If I am in Walla Walla or I am in San Diego and I have a patient that came in from San Francisco to San Diego, I have to reach in to the server that is at your hospital to get the data on that patient. It is not in any central depository where I can go and grab that data as a VA practitioner.

So they made the regional centers, supposedly I thought, as a redundant backup so that if one hospital goes down, you can retrieve that information automatically.

Now something dramatically, intrinsically went wrong with this meltdown. And that is unacceptable. You can't let that happen again.

But the question I ask of you is did that regionalization and centralization happen before General Howard had to inherit that issue? So that was there. That is set up. That infrastructure and that internal control and security was in place.

Now what he had to do was mitigate that. If he has inherited that mess and if there is a problem with it, he is going to have to fix it. And we are going to have to give him the money. These

members are going to have to vote on that. And give him that kind of money to make sure that never happens again.

But the question I have for you is, before centralization, how much down time did you have? Every hospital I know has had their systems crash. Our system in our Committee has crashed for a couple of days at a time where we couldn't retrieve anything.

So when you say that you have more downtime since centralization, and these regional data processing systems were in before centralization, how do you then address that the centralization is the cause of that downtime?

Dr. DAVOREN. I am not sure that centralization in terms of OIT reorganization is the cause of that. Centralization of the resources did create a new point of failure.

And the local facility understanding was, and we have been told this in fact, and there is a memorandum from December of 2006 that I don't have with me, but I can retrieve, that it would be essentially a seamless transition from the Sacramento Regional Data Processing Center for us to the Denver Regional Data Processing Center.

So what I would say is that what you have said is exactly true. But the control on August 31st of moving the plan that we all understood at the field level was that when there was a big catastrophe such as what happened, we would be moved over to the Denver backup. That did not happen. And we did have the longest down—this is the longest unplanned downtime that we have ever had in San Francisco since we have had an electronic medical record.

We have had two planned down times during major system upgrades, well coordinated, incredibly well set up in advance on weekends that were 8 hours in duration. But this was 9 hours for us unplanned. The longest that we have ever had.

Mr. WU. Are you a researcher also?

Dr. DAVOREN. Somewhat. I mostly do clinical work and informatics.

Mr. WU. Are you familiar with the breach at Birmingham in research?

Dr. DAVOREN. Yes.

Mr. WU. Do you have any idea what that is going to cost the VA to mitigate?

Dr. DAVOREN. No.

Mr. WU. What about $26 million? Do you think there should be some personal responsibility of whoever does that?

Dr. DAVOREN. I think that the—one of the good news points that I said before is that the mentality has been a major—a major emphasis of what has gone on with the reorganization in terms of the security initiatives to get people to really pay attention to the level of detail of knowledge that they have about everything that is at our fingertips.

The same quality that makes sensitive information so sensitive is what makes it necessary for us to know it in an instant.

Mr. WU. I appreciate your testimony about, what doesn't need to be encrypted on thumb drives, what is in meetings and presentations. But how do the IT security people know what is on those unencrypted thumb drives?

This is the security event report that comes out every week to Congress, to this Committee, to Chairman Filner and Mr. Buyer. We get them. Not all of them are great. Some are, you know, incidental. Some are—I don't even know why they report them. But they report everything.

For your testimony, what should and shouldn't be encrypted? Who determines that? And is that on a personal recognizance of the physician or the practitioner or the VA employee? How do you then know what is on there? What isn't on there?

We have a report of a cardiologist losing his thumb drive in the Midwest, with 26,000 names on it. What should happen, do you think, to that individual after they certified that they would not do that?

Dr. DAVOREN. Well, I am not as familiar enough with the actual channels for discipline that might be appropriate in such a case. I think that we have made good moves to try and keep people from keeping such information on devices. But, obviously, it can happen. I think everything is, in fact, a risk benefit assessment.

If you encrypt the desktops as has been proposed, if it takes me 25 minutes to get into the data that I need, I am going to tell you as a clinician, I don't believe that is worth it. But the data is much more secure that way. And you will have prevented other people from seeing it even if I can't use it for the veteran in front of me.

So I think everything is about a balance. So I think in order to answer your question, the—how does the information security officer know everything that is on the thumb drive, with current technology, I don't believe there is a way to do so. So I believe that there is a certain amount of policy and procedure that always exists independent of the actual technical action that is taken.

But I think it is just as important that we have the avenues of communication open to be able to discern when those become or appear to be punitive at the end result and when they appear to be completely justified.

But I don't know that I am qualified to tell you exactly what should happen.

Mr. WU. I can appreciate that. And I thank Chairman Filner.

The CHAIRMAN. Thank you, Mr. Wu, for your contributions. I just want to give our counsel a couple of questions. And then we will——

Mr. BESTOR. I don't have a phone book. So I can't read from that. And I wouldn't suggest that Art was doing that either. Sorry.

But actually, Dr. Tibbits, I wanted to ask you a couple of questions about the seamless transfer of information between DoD and VA, because obviously that is a big issue. There a lot of resources being spent on it.

The first thing about the possibility that VistA could be used by DoD, of course, nobody would suggest that you just parachute VistA into DoD. Presumably there would have to be some kind of development of DoD—of VistA to be—to make it possible for DoD to use it.

Clearly there are requirements that DoD has like readiness that the VA—and I keep hearing readiness is the big one. There is a chart on my wall of the information systems in DoD. It is only

eight-and-a-half by eleven. But it has got at least, I don't know, 100–150 different little points on it.

Obviously, there would be a development process that one would have to go through. But it is the case that something like 75 percent of new docs have had some experience on VistA, because they go through a VA rotation during their residencies these days.

And it is also true that a development process might be able to address those. The question is why isn't that being done? I mean, why—what is it about VistA that makes DoD so resistant to even looking at that as the in patient—well, not in patient, as the clinical medical record?

Dr. TIBBITS. Well, that is also a very good question. And there are probably lots of things. So let me—I guess I am going to basically think out loud with you.

I would also, obviously, encourage you to ask DoD that question, because I don't want to speak for them——

Mr. BESTOR. Obviously.

Dr. TIBBITS [continuing]. As to what is in their mind with respect to VistA.

So let me speak about objectives again and start off there. Your preamble included, I think, information sharing or something or serving veterans in—leading into your question.

I would say that were we able to do the development work to put VistA into the Department of Veterans Affairs in some way, shape, or form, might be a very good idea. And I am going to come back to that in a minute. It might be a very good idea and might be feasible.

I just want to go back for a moment, however, to my earlier discussion about email and the Englishman and the Frenchman. Let us not make the mistake that no matter how much development works goes on to put VistA into the Department—into DoD. No matter how much work goes on and if it is feasible, do not make the mistake of believing that that will accomplish information interoperability. It will not. It will do other things.

You mentioned, for example, most doctors who go through training today in the United States in some way, shape, or form go through the VA. True. Therefore, most of them have used VistA. True. And, in fact, most of them like it. True.

Okay. So what would putting VistA in the Department of Defense do today? It would probably reduce the training burden for those doctors over there, because they are already familiar with VistA. It might improve penetration of information technology into healthcare delivery in the Department of—in DoD, because VistA has a much higher success rate with respect to penetration and to healthcare than Alta does in the Department of Defense.

So some very good things might happen by doing that. Just don't put your eggs in that basket with respect to information interoperability between the two departments. It won't accomplish that.

The information interoperability between the two departments has got to deal with the data and how the data goes between the two departments, whether we put VistA over there or not.

Now with respect to some other considerations, let me bring you all around to the notion of templates and structured data. We in the Department of Veterans Affairs right now are beginning more

and more to use templates. We are beginning to use templates for the assessment of patients for the purpose of disability determination. Those are coming largely out of Steve Brown in Nashville with the Compensation and Pension Exam Program initiative. The acronym explanation, which I don't remember. Clinical evaluation, something or other.

Anyway, lots of good work going on with respect to templates there. So we are moving in that direction.

One of the major stumbling points, there are several, but one of the major stumbling points on the Alta side in DoD is that over there doctors hate templates. And the very—one of the high, high, high design objectives of Alta, irrespective of what clinicians in the clinic wanted, was to have machine-readable concepts captured when the clinician put data into the system, the history, the physical, all the unstructured stuff, the text. My chief—I got sick 3 days ago when I hit my head on the door, and so forth, and so forth.

To do all that in machine-readable terminology so that the system could do two things, automatically read that stuff and suggest codes so that the implantable cardioverter-defibrillator and current procedural terminology coding would happen automatically. Could be suggested to the doctor. The doctor attests to the legitimacy of the coding. That is for productivity measurement.

And the second thing is for syndromic surveillance with respect to bioterrorism. So when all those symptoms, I have fever, I have a headache, are in there in machine-readable terms that the computer can understand, the computer can then begin to do epidemiologic surveillance even if the doctor's diagnosis is wrong. It doesn't depend any longer on the doctor's diagnosis, incomplete or wrong, because symptoms can directly be searched. That requires machine-readable data entry, the thesaurus we talked about before.

Well that creates an incredible imposition on physicians with respect to their normal workflow when they are seeing patients. They hate it by and large.

So there is this very interesting sort of debate of objectives, I guess, between the two departments where we are moving toward templates. DoD is figuring out how to move somewhat away from templates. And do a little bit less of it. And where that balance is going to fall, I don't know.

Now let me go to theater. Yes, with respect to military support of medical—I'm sorry, medical support of military operations that is clearly a unique mission the Department of Defense has, which we do not have.

The human form factors of what a computer looks like. Is it a Blackberry? Is it a big machine? Is it a desktop? How big the screen is. Does it operate in the mud? Can it operate in the rain? All those kind of factors. How screen—how fast the screen paint time is.

Communications, in theater, while communications may not be universally available in the United States, it is a whole lot more reliable in the United States than it is in Afghanistan.

So all the applications in Afghanistan have to be modified for unreliable communications. That is a mission the Department of Veterans Affairs does not have.

So when applications are being considered in economies of scale and all that kind of stuff, are both departments really sure that by trying to converge on the application software itself, we are making the best economic decision.

Let me give you an example, a truck. Suppose you had to design a truck that had to operate in the mud effectively and drive efficiently through downtown Washington, DC. I would contend that the form factors on that truck might be such that and something had to pass between the two trucks. Let us say they're both ambulances, and you had to pass patients between the two.

I would contend that a whole lot of engineering analysis would have to go on to determine is one truck with a certain bit of modifications the most efficient way to design this new vehicle so that it works both in the mud, and Afghanistan, and in downtown Washington, DC, or is it cheaper and more effectively to simply design two trucks where the back doors fit each other and we can pass the patient through it?

I would contend that is not a foregone conclusion. And it has to be thought through.

The CHAIRMAN. Actually, Doctor, I can think of a response to that analogy, but I don't want to keep us all here. You and I are going to be talking a lot.

Dr. TIBBITS. Great.

The CHAIRMAN. So we can talk about that some more. You know, it is really about information exchange. It is not—wouldn't you want the same size bolts and all that kind of stuff. But let us not go there.

Let me ask you about this interoperability thesaurus. Tell—the Clinical Data Repository/Health Data Repository (CHDR) the VA is working on, is that the thesaurus work that you are talking about, the updated repository?

Dr. TIBBITS. Yes. That is the thesaurus work on our side.

The CHAIRMAN. Right. And the Clinical Data Repository (CDR) is the thesaurus work on DoD's side, correct.

Dr. TIBBITS. That is correct.

The CHAIRMAN. And we are looking at timeframes that are 8 years out?

Dr. TIBBITS. Could possibly be, which is why I am suggesting we need a simplifying construct to accelerate that work.

The CHAIRMAN. Okay. I am not sure what you mean by "a simplifying construct." You can have interim solutions even if you are continuing to work toward that long-term goal.

Dr. TIBBITS. Exactly right. And——

The CHAIRMAN. And is that what you mean?

Dr. TIBBITS. Yeah. It is what I mean. And those interim solutions, if we focus on information interoperability for the purpose of serving veterans——

The CHAIRMAN. Right.

Dr. TIBBITS [continuing]. And don't distract ourselves at the application software level and worry about what will work in theater and all that stuff. If we don't distract ourselves with that question, focus on the information number one. Number two, focus on what the high-priority problems are today that we need to fix for servicemembers and veterans.

The CHAIRMAN. Right.

Dr. TIBBITS. Traumatic brain injury, PTSD, amputation. What is the information exchange that has to go on between the two departments to optimally handle those conditions?

The CHAIRMAN. Right.

Dr. TIBBITS. That is a list. Some of that list could, in fact, be computable. Some of it may be computable already today. Some of that list might not be computable, but exchangeable today in non-computable fashion, fine.

And some of that list might not yet have been addressed. But could be addressed in a non-computable fashion, so we don't need a thesaurus solution.

The CHAIRMAN. Right.

Dr. TIBBITS. But those layers of composite approaches that I just described could be put in place in an organized manner and plan that would greatly accelerate the information exchange between the two departments. And alleviate as to some extent of this critical path thesaurus work that is going to—it is by definition going to still take a long time.

The CHAIRMAN. Right.

Dr. TIBBITS. One more comment. I would suggest, and I have suggested by the way, the Administration has put a very high priority in VA/DoD collaboration. I assume you all know that. Both the Deputy Secretaries of both departments meet weekly on this subject. I am part of that process with Secretary England and Secretary Mansfield. They have their four-stars in the building meeting with the Undersecretaries, and so forth, and on our side as well.

I have suggested to that group, and DoD has agreed, that we will also undertake another level of assessment with respect to interoperability. And you mentioned the two key elements, the health data repository and the clinical data repository, which today are connected together by a wire over which we transmit standardized data called CHDR.

The CHAIRMAN. Right.

Dr. TIBBITS. CHDR.

The CHAIRMAN. Right.

Dr. TIBBITS. My proposition to the Department of Defense is why don't we simply put a workgroup together, which we now have done by the way. Why don't we put a workgroup together to look at the entire constructive Health Data Repository, the entire constructive of the CDR? See if we can eliminate those two things as two separate constructs and simply create one common database under both medical records.

If we can create one common database under both medical records, then the application software doesn't matter anymore.

The CHAIRMAN. Right.

Dr. TIBBITS. DoD can use their Alta. We could use our VistA. Indian Health Service, if we wanted to, they could use their Indian Health Service applications. If we all put stuff in the same database, we will have achieved the information interoperability objectives we need to serve veterans. And completely end this debate about whose application is better or more suited to the target environment.

The CHAIRMAN. Right. And so what is the timeframe? Suppose tomorrow they say do it. How long does it take to do it?

Dr. TIBBITS. To put those two databases together?

The CHAIRMAN. Yes.

Dr. TIBBITS. I would say it is going to give—I would say it is going to take us probably 6 months to have an answer as to whether it is feasible and will save us time.

My hypothesis is that it will be feasible and it will save us time. That is a hypothesis that remains to be confirmed.

The CHAIRMAN. Okay. And is what you just described doing testing that hypothesis?

Dr. TIBBITS. Yes. That is the study that is going on.

The CHAIRMAN. Okay.

Dr. TIBBITS. Yes. We have launched that study. Yes.

The CHAIRMAN. Thank you very much. I think we have learned a lot. I appreciate your input. You read too much Dr. Seuss, will it work in the mud? Will it work on the scud? Will it work with a lot of blood? His widow lives in my district. So I am going to bring this to her.

But thank you very much. Thank you very much Mr. Wu. Thank you, Mr. Bestor. We have a lot of work. Everybody is impatient. So if you need more resources to go faster, let us know please.

General, do you have anything to add?

General HOWARD. Sure. We just appreciate your support. And we are in constant communication with your staff. And if we need help, rest assured we will come forward.

The CHAIRMAN. Thank you, sir. This hearing is adjourned.

[Whereupon, the Committee was adjourned.]

APPENDIX

Prepared Statement of Hon. Bob Filner, Chairman, Full Committee on Veterans' Affairs

Thank you all for coming here today for this hearing on VA's information technology reorganization efforts. We will examine the progress the VA has made in centralizing its IT efforts.

We shall explore the progress the VA has made in its efforts to be the "gold standard" of information security among Federal agencies, a goal enunciated by Secretary Nicholson in the wake of last year's data breach involving over 25 million veterans and the incident earlier this year in Birmingham, Alabama.

This Committee understands that IT centralization will not happen overnight, nor are we asking it to, but we are asking—and our veterans are demanding—that the VA to be held accountable for getting the job done.

This past June, the Government Accountability Office (GAO), while praising the commitment from senior leadership, found fault with a number of areas in the VA's efforts, areas that hinder the VA's ability to successfully reach its reorganization goals.

They included . . . rejecting GAO's recommendation that VA create a dedicated implementation team responsible for day-to-day management of major change initiatives. Instead, VA is apparently dividing the responsibility among two organizations in the new structure. GAO was concerned that this approach would not work, ***and so is this Committee.***

More recently, GAO reported that of ***17 recommendations made by the VA Inspector General, 16 had not yet been implemented.*** Implementing these recommendations is essential if the VA is to protect private information and meet its obligations under the Federal Information Security Management Act (FISMA).

In the final analysis, we must remember that IT is merely a tool, a tool used by the VA in furtherance of its mission of caring for veterans. This Committee has continued to work in a bipartisan fashion to encourage the VA to centralize its IT efforts. These efforts will lead to concrete benefits for both the VA, taxpayers, and most importantly our veterans.

As we look to the VA to better manage its IT efforts, and to take the lead in data security efforts, we must also ensure these efforts do not unduly harm the VA's mission of providing healthcare and benefits to our veterans.

Our charge is to ensure that while VA is carrying out its mission, it does so with the best and most up-to-date technology the 21st century provides, while securing that technology from outside manipulation and preventing improper disclosure of our veterans' confidential information.

VA, at the same time, must continue the creativity and innovation in the use of electronic medical and other systems that has put VA at the forefront of medical care. These are not easy tasks. We are heartened by many of the steps the VA has undertaken, but remained concerned that more should be done, and could be done . . . ***faster.***

We remain hopeful that the VA can simultaneously provide our veterans the greatest security, management and healthcare. Undoubtedly, the efficient and effective management and operation of the VA IT efforts will realize tangible benefits for our veterans.

Prepared Statement of Hon. Stephanie Herseth Sandlin, a Representative in Congress from the State of South Dakota

Thank you Chairman Filner and Ranking Member Buyer for holding today's hearing to evaluate the VA's reorganization of its information technology infrastructure and management.

Considering the numerous hearings that this Committee dedicated last year to investigating the VA's information technology problems, it is only right that we take

this opportunity to follow-up on the progress of VA's reorganization efforts. This Committee, and Congress as a whole, have a responsibility to remain vigilant in its oversight role to ensure the VA continues to move forward in its pledge to protect the private information of our Nation's veterans.

I share the frustration of my colleagues regarding the repeated failures to change the VA's information organizational structure and the recurring instances of lost personal information.

I thank Mr. Howard and Mr. Claudio for testifying today. I have heard good things about your commitment to providing a secure information technology environment. In order for this Committee to properly conduct its oversight responsibilities we must be able to engage in an open and honest discussion. It is extremely valuable for the Committee to hear from those of you on the frontline working to bring down the institutional barriers of VA's current IT organizational structure.

While the VA has taken important steps toward completing information technology realignment, many questions remain unanswered and many changes to the VA's policies, regarding the handling of sensitive information, will need to be made.

I hope that today's hearing will shed some light on these unanswered questions and lead to better safeguarded information security systems at the VA.

We must work to ensure that the personal information of our Nation's veterans is protected and these widely reported security incidents never happen again.

Thank you again Mr. Chairman. I look forward to hearing from today's witnesses.

Prepared Statement of Hon. Henry E. Brown, Jr., a Representative in Congress from the State of South Carolina

Mr. Chairman and Ranking Member Buyer, thank you for calling this hearing to examine the VA's information technology management structure. I hope that this Committee will take a serious step in addressing one of the biggest challenges facing the Department today; improving the capabilities of VA's information technology system, while strengthening security measures.

As the Congress and this Committee looks at VA's information technology reorganization and the progress that they have made as a result of establishing a centralized management system, I am hopeful that we will do so in a way that focuses on the bipartisan concern we have for the wellbeing of our Nation's veterans. I believe that improving access to healthcare, providing benefits, and implementing information technology go hand-in-hand as we work to ensure that our Nation's veterans have all the resources they need to make a seamless transition into civilian life.

In closing, Mr. Chairman, I look forward to hearing from our witnesses this morning and the discussion that we will have on this important issues. Again, Mr. Chairman, thank you for the time, which I now yield back.

Prepared Statement of Hon. Ginny Brown-Waite, a Representative in Congress from the State of Florida

Thank you Mr. Chairman,

I want to thank all of our witnesses here today for testifying before this Committee. There has been a great deal of focus placed on the use of Information Technology at the Department of Veterans Affairs. The VA relies heavily on information technology to carry out its important mission of serving our Nation's veterans.

The VA undertook an ambitious process to recentralize its IT functions in 2003 and learned many valuable lessons as a result. This has led Secretary Nicholson to approve a federated IT management system for the VA. In this new federated system, the VA divided operations and maintenance from systems development. Innovative thinking like this is needed to ensure that the VA is meeting the needs of veterans in an effective and efficient manner.

Overhauling the IT system at the VA has been a long and difficult process and completion of the realignment is scheduled for July 2008. However, a June 2007, GAO report states, that the VA risks jeopardizing the success of these efforts and may not realize the long-term benefits of the realignment if they do not comply with the recommendations made by the GAO. I look forward to hearing more about these recommendations from both the GAO and the VA here today.

Once again, I welcome you to the hearing and look forward to hearing your thoughts on the issue before us today.

**Prepared Statement of Hon. John T. Salazar,
a Representative in Congress from the State of Colorado**

Thank you Mr. Chairman.

Mr. Chairman, I'm a potato farmer, and in the 30 years that I've been farming I've seen how technology has changed farming operations all over the world.

Change and advancement are inevitable when it comes to technology. It's the nature of the beasts.

A farmer can spend hundreds of thousands of dollars on a single piece of equipment, but unless that farmer knows how to manage that machine and manages it correctly, that tractor will destroy the crops the farmer is attempting to harvest.

We could have the most advanced technology in the world, but it's useless if we fail to manage it properly.

A year ago, we heard about an employee of the VA who had his laptop stolen, potentially compromising the personal records of over 2 million veterans.

Since then, important steps have been taken by the VA to minimize the possibility of these types of things from happening in the future. Some of these steps have been taken voluntarily by the VA and some have been mandated by Congress.

Last year, there were major changes in the management of IT affairs at VA, and this hearing is a chance to get a reading on the impact of that change.

This hearing and the multiple hearings we've had in the last few years like this one are about more than just the IT department in a government agency.

The records being kept by VA belong to real people; men and women who served our country during both times of peace and times of conflict.

I look forward to the testimony from our witnesses. I hope to get a better sense of where the Department is and where it plans to go with the technology it has in its hands.

**Prepared Statement of Valerie C. Melvin, Director,
Human Capital and Management Information Systems Issues,
U.S. Government Accountability Office**

Veterans Affairs—Sustained Management Commitment and Oversight are Essential to Completing Information Technology Realignment and Strengthening Information Security

GAO Highlights

Why GAO Did This Study

The Department of Veterans Affairs (VA) has encountered numerous challenges in managing its information technology (IT) and securing its information systems. In October 2005, the department initiated a realignment of its IT program to provide greater authority and accountability over its resources. The May 2006 security incident highlighted the need for additional actions to secure personal information maintained in the department's systems.

In this testimony, GAO discusses its recent reporting on VA's realignment effort as well as actions to improve security over its information systems. To prepare this testimony, GAO reviewed its past work on the realignment and on information security, and it updated and supplemented its analysis with interviews of VA officials.

What GAO Recommends

In recent reports, GAO made recommendations aimed at improving VA's management of its realignment efforts and information security program.

What GAO Found

VA has fully addressed two of six critical success factors GAO identified as essential to a successful transformation, but it has yet to fully address the other four, and it has not kept to its scheduled timelines for implementing new management processes that are the foundation of the realignment. That is, the department has ensured commitment from top leadership and established a governance structure to manage resources, both of which are critical success factors. However, the department continues to operate without a single, dedicated implementation team to manage the realignment; such a dedicated team is important to oversee the further implementation of the realignment, which is not expected to be complete until July 2008. Other challenges to the success of the realignment include delays in staffing and in implementing improved IT management processes that are to address longstanding weaknesses. The department has not kept pace with its schedule for imple-

menting these processes, having missed its original scheduled timeframes. Unless VA dedicates a team to oversee the further implementation of the realignment, including defining and establishing the processes that will enable the department to address its IT management weaknesses, it risks delaying or missing the potential benefits of the realignment.

VA has begun or continued several major initiatives to strengthen information security practices and secure personally identifiable information within the department, but more remains to be done. These initiatives include continuing the department's efforts to reorganize its management structure; developing a remedial action plan; establishing an information protection program; improving its incident management capability; and establishing an office responsible for oversight and compliance of IT within the department. However, although these initiatives have led to progress, their implementation has shortcomings. For example, although the management structure for information security has changed under the realignment, improved security management processes have not yet been completely developed and implemented, and responsibility for the department's information security functions is divided between two organizations, with no documented process for the two offices to coordinate with each other. In addition, VA has made limited progress in implementing prior security recommendations made by GAO and the department's Inspector General, having yet to implement 22 of 26 recommendations. Until the department addresses shortcomings in its major security initiatives and implements prior recommendations, it will have limited assurance that it can protect its systems and information from the unauthorized disclosure, misuse, or loss of personally identifiable information.

Mr. Chairman and Members of the Committee:

Thank you for inviting us to participate in today's hearing on the Department of Veterans Affairs (VA) realignment of its information technology management structure and actions toward strengthening its information security program. In carrying out its mission of serving our Nation's veterans, the department relies heavily on information technology (IT), for which it expends about $1 billion annually. As you know, however, VA has encountered persistent challenges in IT management, having experienced cost, schedule, and performance problems in its information system initiatives, as well as losses of sensitive information contained in its systems. We have reported that a contributing factor to VA's challenges in managing projects and improving security was the department's management structure, which until recently was decentralized, giving the administrations [1] and headquarters offices [2] control over a majority of the department's IT budget.

In October 2005, VA initiated a realignment of its IT program to provide greater authority and accountability over its resources. In undertaking this realignment (due for completion in July 2008), the department's goals are to centralize IT management under the department-level Chief Information Officer (CIO) and standardize operations and the development of systems across the department through the use of new management processes based on industry best practices. This past June we reported on the department's realignment initiative, noting progress as well as the need for additional actions to be completed. [3] Just last week, we also released a report on VA information security, which included an assessment of the realignment with regard to the department's information security practices. [4]

At your request, my testimony today will summarize the department's actions to realign IT management and our findings regarding the department's information security program. In developing this testimony, we reviewed our previous work on the department's realignment and efforts to strengthen information security. We also obtained and analyzed pertinent documentation and supplemented our analysis with interviews of responsible VA officials to determine the current status of the department's realignment efforts. All work on which this testimony is based was conducted in accordance with generally accepted government auditing standards.

---

[1] The VA comprises three administrations: the Veterans Benefits Administration, the Veterans Health Administration, and the National Cemetery Administration.

[2] The headquarters offices include the Office of the Secretary, six Assistant Secretaries, and three VA-level staff offices.

[3] GAO, Veterans Affairs: Continued Focus on Critical Success Factors Is Essential to Achieving Information Technology Realignment, GAO–07–844 (Washington, D.C.: June 15, 2007).

[4] GAO, Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Longstanding Weaknesses at the Department of Veterans Affairs, GAO–07–1019 (Washington, D.C.: Sept. 7, 2007).

Results in Brief

VA has fully addressed two of six critical success factors we have identified as essential to a successful transformation, but it has not kept to its timelines for implementing new management processes that are the foundation of the realignment. Consequently, the department is in danger of not being able to meet its 2008 targeted completion date. The department has ensured commitment from top leadership and established a governance structure to manage resources, both of which are critical success factors. However, the department continues to operate without a single, dedicated implementation team to manage the realignment; such a dedicated team is important to oversee the further implementation of the realignment. Other challenges to the success of the realignment include delays in staffing and in implementing the IT management processes that are the foundation of the realignment. The department has not kept pace with its schedule for implementing these processes, having missed its original scheduled timeframes. Unless VA dedicates a team to oversee the further implementation of the realignment, including defining and establishing the processes that will enable the department to address its IT management weaknesses, it risks delaying or missing the potential benefits of the realignment.

VA has made progress in strengthening information security, but much work remains to resolve longstanding security weaknesses. The department has begun or has continued several major initiatives to strengthen information security practices and secure personally identifiable information [5] within the department. These initiatives include continuing the department's efforts, as described above, to realign its management structure; developing a remedial action plan; establishing an information protection program; improving its incident management capability; and establishing an office responsible for oversight and compliance of IT within the department. However, although these initiatives have led to progress, their implementation has shortcomings. For example, a new security management structure has been implemented, but improved security management processes have not yet been completely developed and implemented; in addition, the new security management structure divides the responsibility for the department's information security functions between two organizations, with no documented process for the two offices to coordinate with each other. Further, the department has made limited progress in addressing prior GAO and Inspector General recommendations to improve security: although VA has taken steps to address these, it has not yet completed the implementation of 22 out of 26 prior recommendations.

In the reports covered by this testimony, we have made numerous recommendations aimed at improving the department's management of its realignment and information security program. VA has agreed with these recommendations and has begun taking or plans to take action to implement them. If this implementation is properly executed, it could help the department to realize the expected benefits of the realignment, as well as to better secure its information and systems.

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. Over time, the use of IT has become increasingly crucial to the department's effort to provide benefits and services. VA relies on its systems for medical information and records for veterans, as well as for processing benefit claims, including compensation and pension and education benefits.

In reporting on VA's IT management over the past several years, we have highlighted challenges the department has faced in enabling its employees to help veterans obtain services and information more quickly and effectively while also safeguarding personally identifiable information. A major challenge was that the department's information systems and services were highly decentralized, giving the administrations a majority of the IT budget. [6] In addition, VA's policies and procedures for securing sensitive information needed to be improved and implemented consistently across the department.

---

[5] Personally identifiable information, which can be used to locate or identify an individual, includes things such as names, aliases, and Social Security numbers.

[6] For example, according to an October 2005 memorandum from the former CIO to the Secretary of Veterans Affairs, the CIO had direct control over only 3 percent of the department's IT budget and 6 percent of the department's IT personnel. In addition, in the department's fiscal year 2006 IT budget request, the Veterans Health Administration was identified to receive 88 percent of the requested funding, while the department was identified to receive only 4 percent.

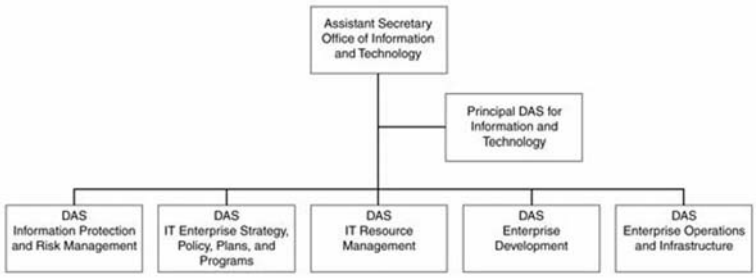
As we have previously pointed out,[7] it is crucial for the department CIO to ensure that well-established and integrated processes for leading, managing, and controlling investments in information systems and programs are followed throughout the department. Similarly, a contractor's assessment of VA's IT organizational alignment, issued in February 2005, noted the lack of control over how and when money is spent.[8] The assessment noted that the focus of department-level management was only on reporting expenditures to the Office of Management and Budget and Congress, rather than on managing these expenditures within the department.

Centralized IT Organization

In response to the challenges that we and others have noted, the department officially began its effort to provide the CIO with greater authority over IT in October 2005. At that time, the Secretary issued an executive decision memorandum granting approval for the development of a new management structure for the department. According to VA, its goals in moving to centralized management are to enable the department to perform better oversight of the standardization, compatibility, and interoperability of systems, as well as to have better overall fiscal discipline for the budget.

In February 2007, the Secretary approved the department's new organizational structure, which includes the Assistant Secretary for Information and Technology, who serves as VA's CIO. As shown in figure 1, the CIO is supported by a principal deputy assistant secretary and five deputy assistant secretaries—new senior leadership positions created to assist the CIO in overseeing functions such as cyber security, IT portfolio management, systems development, and IT operations.

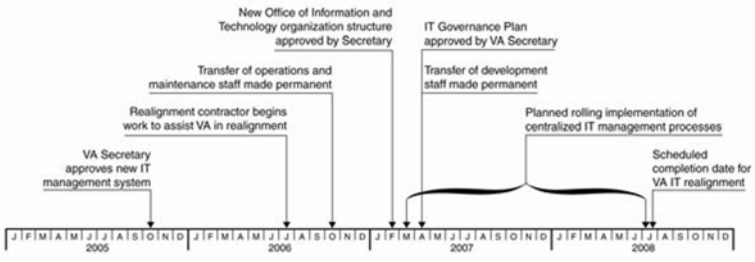
Figure 1—Office of Information and Technology Organizational Chart



Source: VA
Note: DAS = Deputy Assistant Secretary

In addition, the Secretary approved an IT governance plan in April 2007 that is intended to enable the Office of Information and Technology to centralize its decisionmaking. The plan describes the relationship between IT governance and departmental governance and the approach the department intends to take to enhance IT governance. The department also made permanent the transfer of its entire IT workforce under the CIO, consisting of approximately 6,000 personnel from the administrations. Figure 2 shows a timeline of the realignment effort.

Figure 2—Timeline of Key Events for VA IT Realignment



[7] GAO–07–844.
[8] Gartner Consulting, OneVA IT Organizational Alignment Assessment Project "As-Is" Baseline (McLean, Virginia; Feb. 18, 2005).

Multiple Factors Increasing Risk to Success of Realignment

Although VA has fully addressed two of six critical success factors that we identified as crucial to a major organizational transformation such as the realignment, it has not fully addressed the other four factors, and it has not kept to its scheduled timelines for implementing new management processes that are the foundation of the realignment. Consequently, the department is in danger of not being able to meet its target of completing the realignment in July 2008. In addition, although it has prioritized its implementation of the new management processes, none has yet been implemented. In our recent report,[9] we made six recommendations to ensure that VA's realignment is successfully accomplished; the department generally concurred with our recommendations and stated that it had actions planned to address them.

VA Has Not Fully Addressed All Critical Success Factors

We have identified critical factors that organizations need to address in order to successfully transform an organization to be more results oriented, customer focused, and collaborative in nature.[10] Large-scale change management initiatives are not simple endeavors and require the concentrated efforts of both leadership and employees to realize intended synergies and to accomplish new organizational goals. There are a number of key practices that can serve as the basis for Federal agencies to transform their cultures in response to governance challenges, such as those that an organization like VA might face when transforming to a centralized IT management structure.

The department has fully addressed two of six critical success factors that we identified (see table 1).

Table 1—Current Status of VA's Actions to Address Critical Success Factors

Critical success factor	Status as of September 2007
Ensuring commitment from top leadership	**Fully addressed:** Secretary Nicholson approved the new organization structure and the transfer of employees.
Establishing a governance structure to manage resources	**Fully addressed:** Secretary Nicholson approved the IT governance plan, and VA established three new IT governance boards that began meeting earlier this year.
Linking IT strategic plan to organization strategic plan	**Partially addressed:** The department has developed a draft IT strategic plan and expects to finalize it in October 2007.
Using workforce strategic management to identify proper roles for all employees	**Partially addressed:** VA has identified job requirements, has begun to develop career paths for IT staff, and has not yet established a knowledge and skills inventory.
Communicating change to all stakeholders	**Partially addressed:** VA increased communication on the realignment, but has not staffed a key communication office.
Dedicating an implementation team to manage change	**Not addressed:** The department does not have an implementation team to manage the realignment.

Source: GAO.

Ensuring commitment from top leadership. The department has fully addressed this success factor. As described earlier, the Secretary of VA has fully supported the realignment. He approved the department's new organizational structure and provided resources for the realignment effort.

However, the Secretary recently submitted his resignation, indicating that he intended to depart by October 1, 2007. While it is unclear what effect the Secretaries departure will have on the realignment, the impending departure underscores the need for consistent support from top leadership through the implementation of the realignment, to ensure that its success is not at risk in the future.

---

[9] GAO–07–844.

[10] GAO, Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations, GAO–03–669 (Washington, D.C.: July 2, 2003); and Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies, GAO–03–293SP (Washington, D.C.: Nov. 14, 2002).

Establishing a governance structure to manage resources. The department has fully addressed this success factor. The department has established three governance boards, which have begun operation. The VA IT Governance Plan, approved April 2007, states that the establishment and operation of these boards will assist in providing the department with more cost-effective use of IT resources and assets.

The department also has plans to further enhance the governance structure in response to operational experience. The department found that the boards' responsibilities need to be more clearly defined in the IT Governance Plan to avoid overlap. That is, one board (the Business Needs and Investment Board) was involved in the budget formulation for fiscal year 2009, but budget formulation is also the responsibility of the Deputy Assistant Secretary for IT Resource Management, who is not a member of this board. According to the Principal Deputy Assistant Secretary for Information and Technology, the department is planning to update its IT Governance Plan within a year to include more specificity on the role of the governance boards in VA's budget formulation process. Such an update could further improve the structure's effectiveness.

Linking IT strategic plan to organization strategic plan. The department has partially addressed this success factor. VA has drafted an IT Strategic Plan that provides a course of action for the Office of Information and Technology over 5 years and addresses how IT will contribute to the department's strategic plan. According to the Deputy Director of the Quality and Performance Office, the draft IT strategic plan should be formally approved in October 2007. Finalizing the plan is essential to helping ensure that leadership understands the link between VA's organizational direction and how IT is aligned to meet its goals.

Using workforce strategic management to identify proper roles for all employees. The department has partially addressed this success factor. The department has begun to identify job requirements, design career paths, and determine recommended training for the staff that were transferred as part of the realignment. According to a VA official, the department identified 21 specialized job activities, such as applications software and end user support, and has defined competency and proficiency targets [11] for 6 of these activities. Also, by November 2007, VA expects to have identified the career paths for approximately 5,000 of the 6,000 staff that have been centralized under the CIO. Along with the development of the competency and proficiency targets, the department has identified recommended training based on grade level. However, the department has not yet established a knowledge and skills inventory to determine what skills are available in order to match roles with qualifications for all employees within the new organization. It is crucial that the department take the remaining steps to fully address this critical success factor, so that the staff transferred to the Office of Information and Technology are placed in positions that best suit their knowledge and skills, and the organization has the personnel resources capable of developing and delivering the services required.

Communicating change to all stakeholders. The department has partially addressed this success factor. The department began publishing a bimonthly newsletter in June to better communicate with all staff about Office of Information and Technology activities, including the realignment. However, the department has not yet fully staffed the Business Relationship Management Office or identified its leadership. This office is to serve as the single point of contact between the Office of Information and Technology and the administrations; in this role, it provides the means for the Office of Information and Technology to understand customer requirements, promote services to customers, and monitor the quality of the delivered services. A fully staffed and properly led Business Relationship Management Office is important to ensure effective communication between the Office of Information and Technology and the administrations.

Communicating the changed roles and responsibilities of the central IT organization versus the administrations is one of the important functions of the Business Relationship Management Office. These changes are crucial to software development, among other things. Before the centralization of the management structure, each of the administrations was responsible for its own software development. For example, the department's health information system—the Veterans Health Information System and Technology Architecture (VistA)—was developed in a decentralized environment. The developers and the doctors, closely collaborating at local fa-

[11] Competency refers to required capabilities for performing specialized job activities, such as business process reengineering or database administration. Proficiency targets indicate the level at which the individual can perform these activities.

cilities, developed and adapted this system for their own specific clinic needs. The result of their efforts is an electronic medical record that has been fully embraced by the physicians and nurses. However, the decentralized approach has also resulted in each site running a stand-alone version of VistA[12] that is costly to maintain; in addition, data at the sites are not standardized, which impedes the ability to exchange computable information.[13]

Under the new organization structure, approval of development changes for VistA will be centralized at the Veterans Health Administration headquarters and then approved for development and implementation by the Office of Information and Technology. The communications role of the Business Relationship Management Office is thus an important part of the processes needed to ensure that users' requirements will be addressed in system development.

Dedicating an implementation team to manage change. The department has not addressed this success factor. A dedicated implementation team that is responsible for the day-to-day management of a major change initiative is critical to ensure that the project receives the focused, full-time attention needed to be sustained and successful.[14] VA has not identified such an implementation team to manage the realignment. Rather, the department is currently managing the realignment through two organizations: the Process Improvement Office under the Quality and Performance Office (which will lead process improvements) and the Organizational Management Office (which will advise and assist the CIO during the final transformation to a centralized structure). However, the Executive Director of the Organizational Management Office[15] has recently resigned his position, leaving one of the two responsible offices without leadership.

In our view, having a dedicated implementation team to manage major change initiatives is crucial to successful implementation of the realignment. An implementation team can assist in tracking implementation goals and identifying performance shortfalls or schedule slippages. The team could also provide continuity and consistency in the face of any uncertainty that could potentially result from the Secretaries resignation.

Accordingly, in our recent report we recommended that the department dedicate an implementation team to be responsible for change management throughout the transformation and that it establish a schedule for the implementation of the management processes.

Department Is Behind Schedule in Implementing IT Management Processes

As the foundation for its realignment, VA plans to implement 36 management processes in five key areas: enterprise management, business management, business application management, infrastructure, and service support. These processes, which address all aspects of IT management, were recommended by the department's realignment contractor and are based on industry best practices.[16] According to the contractor, they are a key component of the realignment effort as the Office of Information and Technology moves to a process-based organization. Additionally, the contractor noted that with a system of defined processes, the Office of Information and Technology could quickly and accurately change the way IT supports the department.

The department had planned to begin implementing the 36 management processes in March 2007; however, as of early May 2007, it had only begun pilot testing two of these processes.[17] The Deputy Director of the Quality and Performance Office reported that the initial implementation of the first two processes will begin in the second quarter of 2008.

The Principal Deputy Assistant Secretary for Information and Technology acknowledged that the department is behind schedule for implementing the processes, but it has prioritized the processes and plans to implement them in three groups,

---

[12] VA has achieved an integrated medical information system through the use of the Computerized Patient Record System in VistA, where authorized users are able to access patient healthcare data from any VA medical facility.

[13] Computable data are in a format that a computer application can act on, for example, to provide alerts to clinicians (of such things as drug allergies) or to plot graphs of changes in vital signs such as blood pressure. VA has standardized its pharmacy and allergy data in its health data repository.

[14] GAO–07–844.

[15] This official was previously the Director of the IT Realignment Office.

[16] Specifically, these processes are derived from the IT Governance Institute's Control Objectives for Information and related Technology (CobiT®) and Information Technology Infrastructure Library (ITIL) as configured by the Process Reference Model for IT (PRM–IT) from a VA contractor.

[17] These are the risk management and solution test and acceptance processes.

in order of priority (see attachment 1 for a description of the processes and their implementation priority). According to the Deputy Director of the Quality and Performance Office, the approach and schedule for process implementation is currently under review. Work on the 10 processes associated with the first group is under way, and implementation plans and timeframes are being revised. This official told us that initial planning meetings have occurred and primary points of contact have been designated for the financial management and portfolio management processes, which are to be implemented as part of the first group. The department also noted that it will work to meet its target date of July 2008 for the realignment, but that all of the processes may not be fully implemented at that time.

According to the Principal Deputy Assistant Secretary for Information and Technology, the department has fallen behind schedule with process implementation for two reasons:

- The department underestimated the amount of work required to redefine the 36 process areas. Process charters for each of the processes were developed by a VA contractor and provide an outline for operation under the new management structure. Based on its initial review, the department found that the processes are complicated and multilayered, involving multiple organizations. In addition, the contractor provided process charters and descriptions based on a commercial, for-profit business model, and so the department must readjust them to reflect how VA conducts business.
- With the exception of IT operations, the Veterans Health Administration operates in a decentralized manner. For example, the budget and spending for the medical centers are under the control of the medical center directors. In addition, the Office of Information and Technology only has ownership over about 30 percent of all activities within the financial management process. For example some elements within this process area (such as tracking and reporting on expenditures) are the responsibility of the department's Office of Management;[18] this office is accountable for VA's entire budget, including IT dollars. Thus, the Office of Information and Technology has no authority to direct the Office of Management to take particular actions to improve specific financial management activities.

The department faces the additional obstacle that it has not yet staffed crucial leadership positions that are vital to the implementation of the management processes. As part of the new organizational structure, the department identified 25 offices whose leaders will report to the five deputy assistant secretaries and are responsible for carrying out the new management processes in daily operations. However, as of early September, 7 of the leadership positions for these 25 offices were vacant, and 4 were filled in an acting capacity. According to the Principal Deputy Assistant Secretary for Information and Technology, hiring personnel for senior leadership positions has been more difficult than anticipated. With these leadership positions remaining vacant, the department will face increased difficulties in supporting and sustaining the realignment through to its completion.

Until the improved processes have been implemented, IT programs and initiatives will continue to be managed under previously established processes that have resulted in persistent management challenges. Without the standardization that would result from the implementation of the processes, the department risks cost overruns and schedule slippages for current initiatives, such as VistA modernization, for which about $682 million has been expended through fiscal year 2006.

VA Has Much Work Remaining To Resolve Long-Standing Security Weaknesses

Recognizing the importance of securing Federal systems and data, Congress passed the Federal Information Security Management Act (FISMA)[19] in December 2002, which sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. Using a risk-based approach to information security management, the Act requires each agency to develop, document, and implement an agencywide information security program for the data and systems that support the operations and assets of the agency. According to FISMA, the head of each agency has responsibility for delegating to the agency CIO the authority to ensure compliance with the security requirements in the act. To carry out the CIO's responsibilities in the

[18] The Assistant Secretary for Management, who leads the Office of Management, is the department's Chief Financial Officer.

[19] FISMA, Title III, E–Government Act of 2002, Pub. L. No. 107–347 (Dec. 17, 2002).

area, a senior agency official is to be designated chief information security officer (CISO).

The May 2006 theft from the home of a VA employee of a computer and external hard drive (which contained personally identifiable information on approximately 26.5 million veterans and U.S. military personnel) prompted Congress to pass the Veterans Benefits, Healthcare, and Information Technology Act of 2006.[20] Under the act, the VA's CIO is responsible for establishing, maintaining, and monitoring departmentwide information security policies, procedures, control techniques, training, and inspection requirements as elements of the departmental information security program. The Act also includes provisions to further protect veterans and servicemembers from the misuse of their sensitive personally identifiable information. In the event of a security incident involving personally identifiable information, VA is required to conduct a risk analysis, and on the basis of the potential for compromise of personally identifiable information, the department may provide security incident notifications, fraud alerts, credit monitoring services, and identity theft insurance. Congress is to be informed regarding security incidents involving the loss of personally identifiable information.

In a report released last week,[21] we stated that although VA has made progress in addressing security weaknesses, it has not yet fully implemented key recommendations to strengthen its information security practices. It has not implemented two of our four previous recommendations and 20 of 22 recommendations made by the department's inspector general. Among the recommendations not implemented are our recommendation that it complete a comprehensive security management program and inspector general recommendations to appropriately restrict access to data, networks, and VA facilities; ensure that only authorized changes are made to computer programs; and strengthen critical infrastructure planning to ensure that information security requirements are addressed. Because these recommendations have not yet been implemented, unnecessary risk exists that personally identifiable information of veterans and other individuals, such as medical providers, will be exposed to data tampering, fraud, and inappropriate disclosure.

The need to fully implement GAO and IG recommendations to strengthen information security practices is underscored by the prevalence of security incidents involving the unauthorized disclosure, misuse, or loss of personal information of veterans and other individuals (see table 2). These incidents were partially due to weaknesses in the department's security controls. In these incidents, which include the May 2006 theft of computer equipment from an employee's home (mentioned earlier) and the theft of equipment from department facilities, millions of people had their personal information compromised.

Table 2—Number of Incidents by Type Reported to VA's Network and Security Operations Center from January 2003 to November 2006

Type of incident involving the loss of personal information	2003	2004	2005	2006[a]
Records lost or misplaced	19	58	41	316
Records or hardware stolen	7	9	14	65
Improper disposal of records	10	27	10	80
Unauthorized access	60	120	112	255
Unencrypted e-mails sent	8	13	16	170
Unintended disclosure or release	22	48	24	199
Total number of incidents	126	275	217	1,085

Source: GAO analysis of VA data on incidents.
[a]Numbers reported are from January 1, 2006, to November 3, 2006.

While the increase in reported incidents in 2006 reflects a heightened awareness on the part of VA employees of their responsibility to report incidents involving loss of personal information, it also indicates that vulnerabilities remain in security controls designed to adequately safeguard information.

---

[20] Veterans Benefits, Healthcare, and Information Technology Act of 2006, Pub. L. No. 109–461 (Dec. 22, 2006).
[21] GAO–07–1019.

Since the May 2006 security incident, VA has begun or has continued several major initiatives to strengthen information security practices and secure personally identifiable information within the department. These initiatives include the realignment of its IT management structure, as discussed earlier. Under the realignment, the management structure for information security has changed. In the new organization, the responsibility for managing the program lies with the CISO/Director of Cyber Security (the CISO position has been vacant since June 2006, with the CIO acting in this capacity), while the responsibility for implementing the program lies with the Director of Field Operations and Security. Thus, responsibility for information security functions within the department is divided.

VA officials indicated that the heads of the two organizations are communicating about the department's implementation of security policies and procedures, but this communication is not defined as a role or responsibility for either position in the new management organization book, nor is there a documented process in place to coordinate the management and implementation of the security program. Both of these activities are key security management practices. Without a documented process, policies or procedures could be inconsistently implemented throughout the department, which could prevent the CISO from effectively ensuring departmentwide compliance with FISMA. Until the process and responsibilities for coordinating the management and implementation of IT security policies and procedures throughout the department are clearly documented, VA will have limited assurance that the management and implementation of security policies and procedures are effectively coordinated and communicated. Developing and documenting these policies and procedures are essential for achieving an improved and effective security management process under the new centralized management model.

In addition to the realignment initiative, the department also has others under way to address security weaknesses. These include developing an action plan to correct identified weaknesses; establishing an information protection program; improving its incident management capability; and establishing an office to be responsible for oversight of IT within the department. However, implementation shortcomings limit the effectiveness of these initiatives. For example:

- VA's action plan has task owners assigned and is updated biweekly, but department officials have not ensured that adequate progress has been made to resolve items in the plan. Specifically, VA has extended the completion date at least once for 38 percent of the plan items, and it did not have a process in place to validate the closure of the items. In addition, although numerous items in the plan were to develop or revise a policy or procedure, 87 percent of these items did not have a corresponding task with an established timeframe for implementation.
- VA installed encryption software on laptops at facilities inconsistently; however, VA's directive on encryption did not address the encryption of laptops that were categorized as medical devices, which make up a significant portion of the population of laptops at Veterans Health Administration facilities. In addition, the department has not yet fully implemented the acquisition of software tools across the department.
- VA has improved its incident management capability since May 2006 by realigning and consolidating two incident management centers, and made a notable improvement in its notification of major security incidents to U.S.–CERT (the U.S. Computer Emergency Readiness Team), the Secretary, and Congress, but the time it took to send notification letters to individuals was increased for some incidents because VA did not have adequate procedures for coordinating incident response and mitigation activities with other agencies and obtaining up-to-date contact information.
- VA established the Office of IT Oversight and Compliance to conduct assessments of its facilities to determine the adequacy of internal controls and investigate compliance with laws, policies, and directives and ensure that proper safeguards are maintained; however, the office lacked a process to ensure that its examination of internal controls is consistent across VA facilities.

Until the department addresses recommendations to resolve identified weaknesses and implements the major initiatives it has undertaken, it will have limited assurance that it can protect its systems and information from the unauthorized use, disclosure, disruption, or loss.

In our report released last week, we made 17 recommendations to assist the department in improving its ability to protect its information and systems. These recommendations included that VA document clearly define coordination responsibilities for the Director of Field Operations and Security and the Director of Cyber Security and develop and implement a process for these officials to coordinate on the

implementation of IT security policies and procedures throughout the department. We also made recommendations to improve the department's ability to protect its information and systems, including the development of various processes and procedures to ensure that tasks in the department's security action plans have timeframes for implementation.

In summary, effectively instituting a realignment of the Office of Information and Technology is essential to ensuring that VA's IT programs achieve their objectives and that the department has a solid and sustainable approach to managing its IT investments. VA continues to work on improving such programs as information security and systems development. Yet we continue to see management weaknesses in these programs and initiatives (many of a longstanding nature), which are the very weaknesses that VA aims to alleviate with its reorganized management structure. Until the department fully addresses the critical success factors that we identified and carries out its plans to establish a comprehensive set of improved management processes, the impact of this vital undertaking will be diminished. Further, the department may not achieve a solid and sustainable foundation for its new IT management structure.

Mr. Chairman and Members of the Committee, this concludes our statement. We would be happy to respond to any questions that you may have at this time.

Contacts and Acknowledgements

For more information about this testimony, please contact Valerie C. Melvin at (202) 512–6304 or Gregory C. Wilshusen at (202) 512–6244 or by e-mail at melvinv@gao.gov or wilshuseng@gao.gov. Key contributors to this testimony were made by Barbara Oliver, Assistant Director; Charles Vrabel, Assistant Director; Barbara Collier, Nancy Glover, Valerie Hopkins, Scott Pettis, J. Michael Resser, and Eric Trout.

Attachment 1. Key IT Management Processes To Be Addressed in VA Realignment

In the following table, the priority group number reflects the order in which the department plans to implement each group of processes, with one being the first priority group.

Key area	IT management process	Implementation priority group	Description
Enterprise management	IT strategy	2	Addresses long- and short-term objectives, business direction, and their impact on IT, the IT culture, communications, information, people, processes, technology, development, and partnerships
	IT management	2	Defines a structure of relationships and processes to direct and control the IT endeavor
	Risk management	See note a	Identifies potential events that may affect the organization and manages risk to be within acceptable levels so that reasonable assurance is provided regarding the achievement of organization objectives
	Architecture management	2	Creates, maintains, promotes, and governs the use of IT architecture models and standards across and within the change programs of an organization
	Portfolio management	1	Assesses all applications, services, and IT projects that consume resources in order to understand their value to the IT organization
	Security management	2	Manages the department's information security program, as mandated by the Federal Information Security Management Act (FISMA) of 2002
	IT research and innovation	3	Generates ideas, evaluates and selects ideas, develops and implements innovations, and continuously recognizes innovators and learning from the experience
	Project management	1	Plans, organizes, monitors, and controls all aspects of a project in a continuous process so that it achieves its objectives

Key area	IT management process	Implementation priority group	Description
Business management	Stakeholder requirements management	1	Manages and prioritizes all requests for additional and new technology solutions arising from a customer's needs
	Customer satisfaction management	3	Determines whether and how well customers are satisfied with the services, solutions, and offerings from the providers of IT
	Financial management	1	Provides sound stewardship of the monetary resources of the organization
	Service pricing and contract administration	3	Establishes a pricing mechanism for the IT organization to sell its services to internal or external customers and to administer the contracts associated with the selling of those services
	Service marketing and sales	3	Enables the IT organization to understand the marketplace it serves, to identify customers, to "market" to these customers, to generate "marketing" plans for IT services and support the "selling" of IT services to internal customers
	Compliance management	2	Ensures adherence with laws and regulations, internal policies and procedures, and stakeholder commitments
	Asset management	1	Maintains information regarding technology assets, including leased and purchased assets, licenses, and inventory
	Workforce management	2	Enables an organization to provide the optimal mix of staffing (resources and skills) needed to provide the agreed-on IT services at the agreed-on service levels
	Service-level management	2	Manages service-level agreements and performs the ongoing review of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved
	IT service continuity management	1	Ensures that agreed-on IT services continue to support business requirements in the event of a disruption to the business
	Supplier relationship management	3	Develops and exercises working relationships between the IT organization and suppliers in order to make available the external services and products that are required to support IT service commitments to customers
	Knowledge management	3	Promotes an integrated approach to identifying, capturing, evaluating, categorizing, retrieving, and sharing all of an organization's information assets
Business application management	Solution requirements	2	Translates provided customer (business) requirements and IT stakeholder-generated requirements/constraints into solution-specific terms, within the context of a defined solution project or program
	Solution analysis and design	1	Creates a documented design from agreed-on solution requirements that describes the behavior of solution elements, the acceptance criteria, and agreed-to measurements
	Solution build	3	Brings together all the elements specified by a solution design via customization, configuration, and integration of created or acquired solution components
	Solution test and acceptance	See note a	Validates that the solution components and integrated solutions conform to design specifications and requirements before deployment
Infrastructure	Service execution	2	Addresses the delivery of operational services to IT customers by matching resources to commitments and employing the IT infrastructure to conduct IT operations

Key area	IT management process	Implementation priority group	Description
	Data and storage management	3	Ensures that all data required for providing and supporting operational service are available for use and that all data storage facilities can handle normal, expected fluctuations in data volumes and other parameters within their designed tolerances.
	Event management	3	Identifies and prioritizes infrastructure, service, business and security events, and establishes the appropriate response to those events.
	Availability management	3	Plans, measures, monitors, and continuously strives to improve the availability of the IT infrastructure and supporting organization to ensure that agreed-on requirements are consistently met
	Capacity management	3	Matches the capacity of the IT services and infrastructure to the current and future identified needs of the business
	Facility management	1	Creates and maintains a physical environment that houses IT resources and optimizes the capabilities and costs of that environment
Service support	Change management	1	Manages the life cycle of a change request and activities that measure the effectiveness of the process and provides for its continued enhancement
	Release management	1	Controls the introduction of releases (that is, changes to hardware and software) into the IT production environment through a strategy that minimizes the risk associated with the changes
	Configuration management	1	Identifies, controls, maintains, and verifies the versions of configuration items and their relationships in a logical model of the infrastructure and services
	User contact management	3	Manages each user interaction with the provider of IT service throughout its life cycle
	Incident management	2	Restores a service affected by any event that is not part of the standard operation of a service that causes or could cause an interruption to or a reduction in the quality of that service
	Problem management	2	Resolves problems affecting the IT service, both reactively and proactively

Source: GAO.
[a]The department indicated that this process had completed a pilot, but did not assign it to a priority group.

Appendix III: Information on Selected Security Incidents at VA from December 2003 to January 2007

The Department of Veterans Affairs (VA) had at least 1500 security incidents reported between December 2003 and January 2007 which included the loss of personal information. Below is additional information on a selection of incidents, including all publicly reported incidents subsequent to May 3, 2006, that were reported to the department during this period and what actions it took to respond to these incidents. These incidents were selected from data obtained from VA to provide illustrative examples of the incidents that occurred at the department during this period.

- *December 9, 2003: stolen hard drive with data on 100 appellants.* A VA laptop computer with benefit information on 100 appellants was stolen from the home of an employee working at home. As a result, the agency office was going to recall all laptop computers and have encryption software installed by December 23, 2003.
- *November 24, 2004: unintended disclosure of personal information.* A public drive on a VA e-mail system permitted entry to folders/files containing veterans' personal information (names, Social Security numbers, dates of birth, and in some cases personal health information such as surgery schedules, diagnosis, status, etc.) by all users after computer system changes made. All folders were restricted, and individual services were contacted to set up limited access lists.

- *December 6, 2004: two personal computers containing data on 2,000 patients stolen.* Two desktop personal computers were stolen from a locked office in a research office of a medical center. One of the computers had files containing names, Social Security numbers, next of kin, addresses, and phone numbers of approximately 2,000 patients. The computers were password protected by the standard VA password system. The medical center immediately contacted the agency Privacy Officer for guidance. Letters were mailed to all research subjects informing them of the computer theft and potential for identity theft. VA enclosed letters addressed to three major credit agencies and postage paid envelopes. This incident was reported to VA and Federal incident offices.
- *March 4, 2005: list of 897 providers' Social Security numbers sent via e-mail.* An individual reported e-mailing a list of 897 providers' names and Social Security numbers to a new transcription company. This was immediately reported, and the supervisor called the transcription company and spoke with the owner and requested that the file be destroyed immediately. Notification letters were sent out to all 897 providers. Disciplinary action was taken against the employee.
- *October 14, 2005: personal computer containing data on 421 patients stolen.* A personal computer that contained information on 421 patients was stolen from a medical center. The information on the computer included patients' names; the last four digits of their Social Security numbers; and their height, weight, allergies, medications, recent lab results, and diagnoses. The agency's Privacy Officer and medical center information security officer were notified. The use of credit monitoring was investigated, and it was determined that because the entire Social Security number was not listed, it would not be necessary to use these services at the time.
- *February 2, 2006: inappropriate access of VA staff medical records.* A VA staff member accessed several coworkers' medical records to find date of birth. Employee information was compromised and several records were accessed on more than one occasion. No resolution recorded.
- *April 11, 2006: suspected hacker compromised systems with employee's assistance.* A former VA employee is suspected of hacking into a medical center computer system with the assistance of a current employee providing rotating administrator passwords. All systems in the medical center serving 79,000 veterans were compromised.
- *May 5, 2006: missing backup tape with sensitive information on 7,052 individuals.* An office determined it was missing a backup tape containing sensitive information. On June 29, 2006, it was reported that approximately 7,052 veterans were affected by the incident. On October 11, 2006, notification letters were mailed, and 5,000 veterans received credit protection and data breach analysis for 2 years.
- *August 3, 2006: desktop computer with approximately 18,000 patient financial records stolen.* A desktop computer was stolen from a secured area at a contractor facility in Virginia that processes financial accounts for VA. The desktop computer was not encrypted. Notification letters were mailed and credit monitoring services offered.
- *September 6, 2006: laptop with patient information on an unknown number of individuals stolen.* A laptop attached to a medical device at a VA medical center was stolen. It contained patient information on an unknown number of individuals. Notification letters and credit protection services were offered to 1,575 patients.
- *January 22, 2007: external hard drive with 535,000 individual records and 1.3 million non-VA physician provider records missing or stolen.* An external hard drive used to store research data with 535,000 individual records and 1.3 million non-VA physician provider records was discovered missing or stolen from a research facility in Birmingham, Alabama. Notification letters were sent to veterans and providers, and credit monitoring services were offered to those individuals whose records contained personally identifiable information.

**Prepared Statement of Hon. Robert T. Howard,
Assistant Secretary for Information and
Technology and Chief Information Officer,
Office of Information and Technology, U.S. Department of Veterans Affairs**

Thank you, Mr. Chairman. I would like to thank you for the opportunity to testify on the realignment progress in the Office of Information and Technology (OIT).

This is such a crucial issue, and I appreciate the Committee's interest. With me today from OIT is Arnie Claudio (Director, Oversight and Compliance). I am also accompanied by:

- Adair Martinez (Deputy Assistant Secretary for Information Protection and Management)
- Jeff Shyshka (Deputy CIO for Enterprise Operations and Infrastructure)

And on a separate panel will be Paul Tibbits (Deputy CIO for Enterprise Development).

Firstly, I would like to thank you, Mr. Chairman, for giving me the opportunity to testify about the progress being made in OIT's realignment. This Committee has demonstrated great support for and interest in this issue, and we genuinely appreciate it.

Last week, during a similar hearing conducted by the Senate Committee on Veterans' Affairs, I began by talking about my top seven priorities as Assistant Secretary for the Office of Information and Technology. Today, I would like to do that again as these priorities are guiding the realignment process we see taking place. Briefly, they include (1) establishing a well-led, high-performing, IT organization that delivers responsive IT support to the three Administrations and Central Office staff sections; (2) standardizing IT infrastructure and IT business processes throughout VA; (3) establishing programs that make VA's IT system more interoperable and compatible; (4) effectively managing the VA IT appropriation to ensure sustainment and modernization of our IT infrastructure and more focused application development to meet increasing and changing requirements of our business units; (5) strengthening data security controls within VA and among our contractors in order to substantially reduce the risk of unauthorized exposure of veteran or VA employee sensitive personal information; (6) creating an environment of vigilance and awareness to the risks of compromising veteran or employee sensitive personal information within the VA by integrating security awareness into daily activities; and (7) remedying the Department's longstanding IT material weaknesses relating to a general lack of security controls. I assure you that we are working hard to give these priorities the required attention.

As you know, the Government Accountability Office (GAO) recently released a report on our realignment progress and correctly identified that there is more work to be done to have a successful transition from a decentralized to a centralized organization. We have already begun implementing some of their recommendations such as establishing an IT governance plan, continuing with process development, and expediting the development of performance metrics to track realignment progress. Implementing these recommendations will certainly aid in the realignment.

We have made, I believe, solid progress in other areas of this realignment. We have dramatically improved incident response because of the significant amount of policy guidance and training conducted on information protection. Since we have begun this, we have seen an increase in self-reporting security and privacy violations and incidents. We are also making great improvements in the area of data protection by encrypting over 18,000 laptops, implementing procedures for issuing encrypted portable data storage devices, purchasing software to address the encryption of data at-rest this month, reducing the use of Social Security numbers, and reviewing and eliminating a significant amount of personally identifiable information VA currently holds. Regarding these last two points, VA has drafted two documents outlining plans to achieve both these goals. These plans were developed in accordance with the Office of Management and Budget (OMB) Memorandum M–07–16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" and will be included in this year's Federal Information Security Management Act (FISMA) report. Regarding the FISMA report, not only will we submit one this year, (we got an incomplete last year), but we have, for the first time, completed testing of over 10,000 security controls on our 603 computer systems. Mr. Chairman, you will be pleased to know that we recently awarded a contract for extensive port monitoring, which will help us better control network access—a very important tool in our information protection toolkit.

Through this realignment, we are also addressing the critical issue of asset management. As you remember, the House Veterans' Affairs Oversight and Investiga-

tions Committee recently held a hearing on VA's IT asset management based on a GAO report (report 07–505) which found inadequate controls and risk associated with theft, loss, and misappropriation of IT equipment at selected VA locations. In that report, GAO found many problems regarding the IT asset management environment and included a number of important recommendations—with which we agree and are implementing. We have completed a handbook on the Control of Information Technology Equipment within the VA which includes each of the recommendations made by GAO in its report. These documents are now being finalized within the Department, but we have already implemented the procedures they describe. They will provide clear direction on all aspects of IT asset management.

For the past 6 months, tightening IT inventory control throughout VA has been the focus of a cross-functional Tiger Team. In addition, VA has issued a memorandum requiring each VA facility to complete, by the end of December of this year, a wall-to-wall inventory of all IT equipment assets, including sensitive items, regardless of cost. Reporting requirements have been established at the Facility, Regional and Field Operations levels to ensure that issues are identified and addressed early in the process. By way of support, we have established an IT Inventory Control Knowledge Center that is accessible by all VA personnel. This website provides references, templates, definitions, frequently asked questions and a link to contact the Tiger Team directly. Also, the Office of Oversight and Compliance is working with Tiger Team members to develop a compliance checklist that will be used for scheduled and unscheduled audits regarding IT assets. This initial inventory will help provide a VA IT asset baseline—something that has not existed before and is a direct result of the realignment.

Lastly, an important and fair question to ask regarding this realignment is how has it impacted the delivery of healthcare and benefits to our veterans. In my opinion, there has been no significant change in these two areas—which was a key objective of this reorganization—to do no harm. This is not to say we have not had problems—we have. But we have also experienced improvements in our ability to gain knowledge over IT activities that were not very visible in the past, in IT funding details across the VA, and in our ability to protect the sensitive information of our veterans.

In closing, I want to assure you, Mr. Chairman, that a successful realignment in OIT is a key goal within the VA. I have good people in my office who all share this commitment and work hard to achieve it. We have accomplished many things this past year but more remains to be done. I appreciate having this opportunity to discuss this with you and will gladly respond to your questions.

Prepared Statement of Arnaldo Claudio
Executive Director, Office of IT Oversight and Compliance
Office of Information and Technology, U.S. Department of Veterans Affairs

Thank you, Mr. Chairman and Members of the Committee. I appreciate the opportunity to speak with you today on the topic of the Department's Information Technology (IT) reorganization and to share with you the impact and progress that the Department of Veterans Affairs (VA) has achieved as a result of the establishment of the Office of IT Oversight and Compliance (ITOC).

ITOC was established in February of 2007, as a response to the need for the VA to enhance the protection of our veterans' sensitive information. This concept was initially addressed by Professor Eugene H. Spafford, during his Congressional testimony shortly after the data breach of May 2006; and later by the IBM study in their December 2006 publication entitled: *High Level Target Organizational Structure* on VA's IT realignment. Furthermore, in February of 2007, Secretary Nicholson conveyed a strong message regarding the importance of proactively identifying, addressing and mitigating any risks that could jeopardize the potential loss of veterans' sensitive information.

To fulfill this vital requirement, ITOC is charged with providing independent, objective, and quality oversight and compliance assessment services in the area of information and technology to include Cyber Security, Records Management, Privacy and Physical Security.

The concept of ITOC is not entirely new to VA. Prior to ITOC's establishment, a smaller scale initiative collocated within the Office of Cyber and Information Security (OCIS) known as the Review Inspection Division (RID) existed.

In October 2002, the RID was created to fulfill the requirements set by the Office of Management and Budget (OMB), VA Directive 6210, VA policy and Departmental commitments to Congress, which mandated security audits (reviews and inspec-

tions) be conducted at every VA facility on a recurring basis. Although RID was given a mission to review the entire Department's cyber and information security program at all VA facilities, it was never given sufficient resources and authority to carry out all but a small fraction of these tasks. Staffing was inadequate with only five VA employees and a handful of contractors. Considering VA has over 1200 sites, RID was given an impossible task to perform. In addition, none of the detailed reports created and forwarded to OCIS senior management were approved or forwarded to sites.

Today with the establishment of ITOC, that is no longer the case. We are now resourced and equipped to identify issues and to address our observations immediately after the completion of our assessments with the hospital leadership including the facility Director, Chief Information Officer, Information Security Officer, Privacy Officer and other important members of the hospital staff; and thereafter, we report our findings directly to the VA CIO Mr. Robert Howard. The ITOC has the robustness and appropriate strategic planning, focus, and vision necessary to successfully address the new paradigm facing VA.

Since its creation earlier this year, ITOC has grown from 7 to 128 employees and, by the end of Phase 2 in FY 2009, it is expected to have a total workforce of 165 employees. This is in itself a success story. Most government programs take years before they can be stood up and become fully operational. Our employees have been selected from a pool of talented subject matter experts from both industry and government.

The ITOC has achieved a great deal in just a few months and it is already showing dramatic results and measurable benefits across VA. As of today, we have conducted over 100 assessments—a rate of 18 to 20 assessments per month, versus 2 per month compared to our predecessor organization.

We have experienced our share of significant challenges—but none so far that have proven impossible. The assessments performed by my staff are very thorough. We are working together with VHA, VBA and NCA to correct and eliminate the existing deficiencies found by the Inspector General (IG) and the General Accounting Office (GAO) over the last few years.

As Executive Director, for the Office of IT Oversight and Compliance at VA, but first and foremost, as a veteran, I truly feel the responsibility for ensuring compliance with the integrity and security of VA's sensitive information and IT assets. I understand that security awareness is a paradigm change—a change to our business operations culture and simply the way we do things. My staff and I have found that the field facilities welcome our independent and objective assessments as the leadership across VA continues to drive home, to each employee, the importance of securing sensitive information. I am prepared to answer your questions today about what the Office of IT Oversight and Compliance is doing to effect real change to improve VA's FISMA scorecard, as well as how we are working together with other VA Administrations to mentor, train, coach and optimize our valuable resources to better serve our Nation's veterans.

In closing, I want to assure you, Mr. Chairman, and the members of this Committee that we will continue to be diligent in our efforts to improve and remedy VA's Information Technology environment. Thank you for your time and the opportunity to speak on this issue. I would be happy to answer any questions you may have.

Prepared Statement of Paul A. Tibbits, M.D.
Deputy Chief Information Officer, Office of Enterprise Development
Office of Information and Technology, U.S. Department of Veterans Affairs

Thank you, Mr. Chairman. I would like to thank you for the opportunity to testify on the realignment progress in the Office of Information and Technology (OIT) and to share with you the progress made in VA as a result of the centralization of IT development activities.

Joining me on this panel is Dr. Ben J. Davoren, Director, Clinical Informatics, from our San Francisco Medical Center.

This Committee has demonstrated great support for and interest in IT in the VA, and we genuinely appreciate it.

You have just heard testimony from Assistant Secretary Howard regarding the GAO report on our realignment progress and the need for more work to be done to achieve successful transition from a decentralized to a centralized organization. While General Howard focused on the information protection aspects of the realignment, I would like to share with you our progress in establishing an IT governance

plan, strengthening development process improvement efforts, and fostering innovation.

You have also heard General Howard refer to his seven (7) priorities and how they are guiding the realignment process. I would like to talk more about those priorities that have special significance to the Office of Enterprise Development. They include (1) establishing a well-led, high-performing, IT organization that delivers responsive IT support to the three Administrations and Central Office staff sections; (2) standardizing IT infrastructure and IT business processes throughout VA; (3) establishing programs that make VA's IT system more interoperable and compatible; (4) effectively managing the VA IT appropriation to ensure sustainment and modernization of our IT infrastructure and more focused application development to meet increasing and changing requirements of our business units.

CIO Priorities

First, with respect to establishing a well-led, high-performing IT organization that delivers responsive IT support to the three Administrations and Staff Offices, we are pursuing improvement of the development workforce throughout the Office of Enterprise Development. In so doing, development staff will be better prepared to act as knowledgeable consultants at the local level to assist healthcare providers in development of innovation software solutions that are likely to be technically sound and ready for national deployment.

To improve the capability of the VA IT development workforce we are instituting real-time coaching and mentoring by industry experts in best practices for systems development, to institutionalize these practices at the VA.

Improving workforce capability increases the staff's readiness to perform critical development processes, increases the likelihood of achieving desired results from performing the processes, and allows the VA to realize the benefits from the investment in process improvement for all VA facilities.

Second, with respect to standardizing IT infrastructure and IT business processes throughout VA, standardization of these processes provides the baseline for measuring the effectiveness of its development process. It is the first step to reduce time to deliver applications, reduce costs to develop applications, implement business-driven process performance measures, and increase productivity of the development workforce. And it is hard work.

For the IT development organization, our standardized processes are based on industry best practices as codified in the Capability and Maturity Models from the Software Engineering Institute for both software development and workforce competency. We are using independent industry to guide us through this self-improvement initiative.

Third, let me address establishing programs that make VA's IT system more interoperable and compatible. Interoperability begins with a common understanding of terminology. To establish this with sufficient precision, the IT development organization is collaborating closely with the Administrations in use of business modeling to provide a uniform basis of developing a shared understanding of new way to serve veterans and the information required to do so.

Next we are engaging with the Administrations and with DoD to strengthen and accelerate data standardization activities within VA and with DoD. We are exploring ways to focus on high priority patient groups, such as traumatic brain injury and post traumatic stress disorder, while continuing the hard work of semantic analysis and reconciliation and the consolidation of multiple data feeds between VA and DoD.

Fourth, we are focused on managing the VA IT appropriation to ensure sustainment and modernization of our IT infrastructure and more focused application development to meet increasing and changing requirements of our business units. We are applying life cycle and total cost of ownership management practices to all development projects, to account for all costs of implementation and operations, as a foundation for budget formulation. We are moving toward clear, line-of-sight alignment with the VA strategic plan and the Performance Accountability Report by reshaping our OMB 300 exhibits in FY 2010, creation of the first multi-year IT budget, and strengthening our relationship with the requirements processes of the Administrations and Staff offices.

Governance

We have established a participative, transparent IT governance process at the senior executive level of the VA. Decisionmakers at the VA were not equipped with the framework for understanding the relative importance of one dimension of project performance with respect to others, leading to a bias toward financial metrics during process prioritization. Decisionmakers lacked key information with respect to

project benefits and total cost to make effective decisions on priorities. We have created a set of organizational principles and governance structures and practices that surface business strategy; facilitate accurate project cost, benefit, and risk estimation, and provide a decisionmaking framework that focuses attention on a subset of the most critical projects and delivers timely, accurate information to the VA's senior decisionmakers.

We are strengthening the use of earned value systems in our large programs. We have undertaken independent assessment of the soundness of our approach to managing certain IT development projects and will expand this activity.

We are developing management dashboards to implement early warning of issues with system development:

- **Project/program Status**—tracking of project performance as compared to cost, schedule, and scope estimates.
- **Project/program data quality**—Assesses the quality of software releases, through analysis of defects found and problems noted.
- **Project/program Return on Investment (ROI), earned value, and risk management**—Compares real program ROI with estimated ROI, and uses earned value to serve as a leading indicator of deviation from forecasted cost and schedule.
- **Portfolio resource allocation**—Determines the application of financial resources to various projects, to balance production across multiple related initiatives.
- **Portfolio timelines**—Provides an integrated view of program timelines, highlighting the programs that will attain significant milestones or be complete by a specific future date.
- **Portfolio mix**—Displays the mix of project spending among groups of related software applications.

We are focusing intense effort on managing the execution of funds in accordance with established plans, to ensure projects are adequately resourced, and learning lessons for improvements next year.

Promote innovation

Challenges. The Secretary has migrated all IT activities under a single leadership authority, in part due to the need to drive standardization and interoperability of applications and infrastructure across VA. We need application development plans that employ industry best practices and have the potential to accelerate the successful completion of IT projects, including implementation across the VA.

The centralized IT budget (the single IT appropriation) sets a context for competition among new ideas, since some are not affordable. This creates the perception at the hospital that many good ideas are disregarded despite "local needs", and that the flexibility available to VISN and hospital directors to use healthcare funds for IT is a constraint. This view disregards the rest of the story. Solutions developed locally were rarely deployed across all VA medical centers, resulting in some centers not getting the advantage of these IT capabilities. Furthermore, many needs were thought of as local, when in fact they were enterprise-wide requirements, such as reports to support Joint Commission accreditation visits.

Under the single IT authority and single IT appropriation, we operate in an environment of financial transparency. Funds dedicated to sustainment, extending legacy systems to meet urgent needs of returning warriors, and to modernize our computing environment are now visible to senior VA executives. We have no formal mechanism to allocate funds to IT innovation. Unmanaged local innovation makes the implementation of enterprise solutions very difficult. Many IT products are operating in various VAMCs, with no support mechanism to proliferate the more successful of them to all other medical centers.

In close collaboration with VHA, we are moving to create a mechanism to deal with this challenge. We have developed a process to identify new ideas at the local level, facilitate collaboration among field developers and VAMC healthcare professionals, to develop new software products in a non-production environment in an unconstrained manner. In order to enter the live production environment and assure deployability across all VA sites, certain technical, business value, security, and patient safety assessments will be made and any remediation necessary applied. There are effectively no constraints on the trail development of new IT solutions; there are disciplined assessments prior to VA-wide implementation to assure safety and continuity of operations of the IT production environment.

The migration from the VistA legacy system to the Health*e*Vet platform entails complex development, a new programming medium, a new architecture, and establishment of a veteran-centric medical record versus the facility-centric nature of

VistA. This form of innovation must be centrally managed. It is too large for local initiatives alone to accomplish. In addition, some forms of new IT support require an analysis of end-to-end processes to serve veterans, such as transition from DoD to VA, again not easily accomplished at the local level when complex data standardization and security issues are involved. We are attempting to strike the right balance.

Effective communication is critical to successful organizational change. The migration of IT development personnel under a single IT authority will need to be supported by a focused communications strategy and plan to avoid disruption to VA's business operations and to achieve the benefits of new organization.

We are strengthening our communications strategy for the development staff.

There has been no significant change in the delivery of healthcare and benefits to veterans with this realignment. We have had some problems, but we have also gained valuable visibility over unknown IT activities—a definite improvement. We also now know more about IT funding details across the VA and have a greater ability to protect the sensitive veterans' information.

In closing, let me say that we want your ideas. I want to assure you, Mr. Chairman, that a successful realignment of IT development activities is a key goal within the VA. We have accomplished many things this past year but more remains to be done. I appreciate having this opportunity to discuss this with you and will gladly respond to your questions.

Prepared Statement of J. Ben Davoren, M.D., Ph.D.,
Director of Clinical Informatics,
San Francisco Veterans Affairs Medical Center,
Veterans Health Administration, U.S. Department of Veterans Affairs

Good morning, Mr. Chairman and Members of the Committee. Thank you for this opportunity to provide my personal perspective of the Veterans Affairs Office of Information and Technology (OI&T) reorganization that began in 2005. The views that I present today are my own and do not necessarily represent the views of the VA Medical Center San Francisco, Veterans Integrated Service Network (VISN) 21, or the Veterans Health Administration.

I would like to preface my testimony with VHA and OI&T's mutual goals, and principles in the facilitation of the reorganization. In addition, the testimony will discuss realignment concerns I believe were voiced from the field in 2005, my views of the impact of the realignment on Veterans Health Administration's (VHA) missions, and the regional computer system downtime of August 31, 2007, as a paradigm.

Mutual Goals and Principles

As described in a GAO interim report of June 2007, the primary goals of the OI&T reorganization were to centralize IT management under a department-level Chief Information Officer, to standardize operations, and the development of systems across the Department using new management processes based on industry best practices. The VA Inspector General reported that the lack of a centralized structure was a major impediment to successful IT management. Events related to the loss or potential loss of sensitive information reinforced VA's need to reorganize IT, especially in terms of data security processes.

The OI&T stated principles for the reorganization process were that:

- A single IT leadership management system would facilitate achievement of enterprise strategic objectives, standardization, compatibility, interoperability, and fiscal discipline;
- A process-focused organization and IT management system would be aligned with best practices for IT processes, roles, metrics, and governance;
- Strong integration between OI&T and the business offices (VHA, Veterans Benefit Administration, National Cemetery Administration, and Staff Offices) would set IT strategy, determine requirements, and implement solutions;
- Approaches to legacy and new application development would be synchronized;
- New process-based organizational structure for the Office of the Assistant Secretary for Information and Technology would be defined; and
- IT realignment would transform VA into a service-based IT organization with a client-centric IT model that aligned IT with VA business needs, priorities, and mission.

Concerns Voiced From the Field in 2005

In response to the Secretaries proposals for IT realignment, I believe that employees at some medical centers expressed a number of concerns about the details of the plan. In particular, I believe they felt that the regionalization of IT resources would create new points of failure that could not be controlled by the sites experiencing the impact, and that the system redundancy required to prevent this was never listed as a prerequisite to centralization of critical patient care IT resources. From my point of view as the Director of Clinical Informatics, it was clear to me that the focus of reorganization/realignment was on technical relationships and not on how the missions of VHA would be communicated to the new OI&T structure. For example, realignment success metrics were focused on Regional Data Processing Center (RDPC) deliverables rather than facility needs. Finally, key facility-based IT staff had been tightly integrated into local Committees and planning groups as subject matter experts, but could no longer be tasked directly by the facility Director to participate, and had no clear OI&T-driven incentive to continue. Ultimately, the concern was that in trying to create a new structure in the name of "standardization", support would wane to a "lowest common denominator" for all facilities, no matter how diverse their actual needs were.

Impact on VHA's Four Principal Missions

With respect to the primary patient care mission, the good news has been that new policies and procedures regarding encryption of sensitive information have been well-publicized and have heightened the awareness of all care providers as to the critical nature of the information they use everyday. I think this has positively impacted the culture of VHA and improved respect for our veterans. The bad news is that centralization of physical IT resources to the RDPCs has directly led to more system downtime for individual medical centers than they have ever had before, resulting in hundreds of simultaneous threats to the safety of our veteran patients. In addition, it is my opinion that disagreements over whether new proposals for clinical application or device procurement are "IT" or "not-IT" has markedly delayed upgrading of aging systems and implementation of new systems for veterans' care.

With respect to the education mission, the good news is again that standards for encryption of sensitive information have heightened the awareness of all staff and students as to the critical nature of the information they have at their fingertips and the need to protect it in all settings.

However, from my vantage, rules on encryption of all portable devices, such as "thumb drives", rather than just on encrypting sensitive information, have made it cumbersome to go about common work, such as giving academic and scientific presentations where no sensitive information is present. Further, security rules for using network resources have stopped some Internet-based videoconferencing activities between VA and non-VA colleagues, while awaiting new funding cycles to procure next-generation equipment.

With respect to the research mission, the proposed standardization of VHA databases as part of centralization may create significant research opportunities, and has been supported by the research community though, at this time, no specific progress has been made. Rules regarding encryption of transported sensitive information have been warmly received by the research community as a best practice. However, security rules for using network resources have stopped some Internet-based videoconferencing activities between VA and non-VA colleagues. Some additional unique local IT resources have been required to maintain other research activities which utilize the Internet and I have concerns about how long they can continue.

In terms of our role in supporting the Department of Defense, I believe that initiatives to enhance electronic data-sharing between VHA and DoD have proceeded appropriately.

Impact on VHA's Accomplishments and Morale

In my opinion, confirmed in many conversations with my peers, there has been a lack of transparent communication between VHA and the reorganizing OI&T structure. At present, economies of scale that were a cornerstone of the OI&T realignment proposal have not been communicated to the facility level where the work of VHA occurs. The focus on security and data integrity has led to a number of new requirements with impacts that generate significant concern without a clear pathway to resolution. For example, to fully comply with security requirements on our examination room PCs, we must log out of both a clinical application such as our Computerized Patient Record System and the Microsoft Windows operating system each time we leave the room even for a moment, yet it may take as long as 12 minutes to log back on when we return. Given a 20 or 30 minute visit with their vet-

eran patient, the clinician is thus forced to choose to "do the right thing" for either the patient or the system, but cannot do both.

In my view, there remains a tremendous uncertainty about how to work with our longstanding IT colleagues to address local or regional clinical care, research, or educational needs. These arise on an almost daily basis as the result of new mandates from accrediting bodies, VA performance measures, or Congressional action. Accountability for all these activities remains with the individual Facility Directors, but they no longer have the authority to task IT staff nor directly acquire technological resources that are a part of every new idea that is put forth to meet the new needs. There is a sense of great inertia that overrides the anticipation of great opportunities in the new OI&T structure. I believe that this has greatly slowed the field development process that is the very foundation of our VA-created computer system, VistA.

Regional Computer System Downtime of August 31, 2007

On August 31, 2007, the new "Region One" of OI&T-supported facilities experienced the most significant technological threat to patient safety VA has ever had—a 9-hour downtime during standard business hours that crippled the clinical and other information systems of 17 different VHA medical facilities. During the downtime, it became clear to me that many assumptions about the RDPC model were erroneous. Specifically, rather than creating a redundancy to protect facilities from system problems, a new single point of failure caused a problem that could never have been replicated without the RDPC model having been created. In this vein, the ability to "failover" from the RDPC in Sacramento to Denver, previously described as a major advantage to the RDPC model, was never taken advantage of. Electronic contingency systems, put in place as a part of the RDPC migration strategy, were unavailable or overwhelmed in four of the medical centers, despite prior experience that this was a known risk during the pilot phase of the RDPC collocation project. Lastly, and of great concern to the medical centers as a harbinger of future support, clinical need was expected to be the driver of the service restoration process. Instead, half a day of troubleshooting and error log evaluation and analysis went by before the shutdown and reboot process was initiated to actually fix the problem.

The after-action report, while done in a timely fashion and generally clear, did not address the two major concerns of the facilities that had to deal with the impact of the downtime at all. Specifically, how it could be that the RDPC model designed for redundancy could instead have been designed to create the single point of failure that facilities predicted 2 years earlier would paralyze them? Why was the "failover" from the Sacramento RDPC to the Denver RDPC not initiated immediately when the magnitude of the impact was known? Despite repeated queries about this on the official Region 1 VistA Outlook email thread designed to facilitate communication between OI&T and VHA facilities, I am unaware of whether this question was ever answered.

In my view, the OI&T realignment process begun in VA in 2005 for the right reasons has been focused on technical IT issues and the reporting structure of its new 6000-strong employee force. While there has been measurable success in those areas, my perspective is that this has not been the case for the planned linking of IT strategic planning with organizational strategic planning and communication between all stakeholders in VA. Mr. Chairman this concludes my statement. I will be pleased to answer any questions that you or other Members of the Committee might have.

Statement of Hon. Harry E. Mitchell,
a Representative in Congress from the State of Arizona

Thank you Mr. Chairman.

Last week, the Government Accountability Office released their review of the progress made in reorganizing information technology at the VA.

In October 2005, the VA began centralizing its information technology management structure.

Shortly thereafter, in May 2006, a laptop theft from an employee's home containing personal information brought the importance of this issue to light, and the Department's mismanagement of the situation showed the urgency of centralization.

The GAO report showed that the Department has not yet implemented full security protocols to protect veterans' and medical providers' personal information.

It also highlighted the importance of an implementation team, which has also been previously suggested and ignored by top officials in the Department.

Information security is not an issue that we can take lightly these days.

Securing the personal information of our veterans should be a high priority, and any breach of government security should be taken seriously.

Following the compromised security of information at the VA in May of 2006, officials pledged stronger action, but the security breach this past January shows that they have yet to deliver once again.

Arizona leads the nation in identity theft and this report only further concerns me about security at the VA.

I look forward to hearing how we can work together to address this pressing issue.

Statement of Bryan D. Volpp, M.D.,
Associate Chief of Staff, Clinical Informatics,
Veterans Affairs Northern California Healthcare System,
Veterans Health Administration, U.S. Department of Veterans Affairs

Good morning Mr. Chairman and Members of the Committee. Thank you for this opportunity to discuss the impact on patient care due to the disruption to the VISTA and Computerized Patient Record System (CPRS) at the VA Northern California Healthcare System (VA NCHCS). The VA NCHCS is an integrated healthcare delivery system serving more 377,700 veterans dispersed over a wide area covering ten geographic sites. We serve approximately 70,000 unique veterans per year and average close to 2000 visits per day. VA NCHCS offers a comprehensive array of medical, surgical, rehabilitative, primary, mental health and extended care to veterans in Northern California. In addition, we provide inpatient acute and critical care services at the Sacramento site (50 beds) and inpatient nursing home and subacute care (115 beds) at the Martinez site.

Disruption to VISTA and CPRS

On August 31, 2007, at approximately 7:30 am on Friday, VA NCHCS experienced a major disruption with the logons to our VistA and CPRS. The disruption resulted from a problem at the Sacramento Regional Data Processing Center (SRDPC) and affected 17 sites within VA NCHCS.

Contingency Plan for Disruptions

VA NCHCS immediately implemented our local contingency plan for failure, which consists of three backup levels. The first level backup is a switch over from the Sacramento Data Center to the Denver Data Center. The second level backup is a read-only version of the patient data. And the final level of backup is a set of files stored on some local PCs that contains brief summaries of a subset of the patient data for patients who are current inpatients or who have appointments in the next 2 days. A key element in our contingency plan is that communication to the users on the cause and an estimate of length of the downtime are to be made on a regular basis by IRM. This did not occur.

The contingency plans failed to stop the disruption. The switch over to the Denver Data Center did not occur. The read-only backup of the patient data had been made unavailable earlier in the week of August 31 in order for the Regional Data Center staff to create a new version of our test account. Test accounts are required to be refreshed every 4–6 months at all VA sites. With failure of the first two backup levels, we became reliant on the data stored on several local personal computers that could be printed. The data stored on the personal computers are health summaries. Health summaries are brief extracts of the record for patients with scheduled appointments which contain recent labs, medication lists, problem lists and recent notes along with allergies and a few other elements of the patient record. The disruption severely interfered with our normal operation, particularly with inpatient and outpatient care, and pharmacy.

Disruption Impact on Inpatient Care

The inpatient sites were immediately affected. The residents on rounds in all the impacted facilities were not able to access patient charts to review the prior day's results, add or review orders. Nursing reports were interrupted because some of the handoffs from one shift to the next are done by reviewing activities and progress in the electronic record. Discharge planning for that morning was interrupted as well due to lack of electronic record availability. On the inpatient wards, there were many delays in medication administration and in discharges. The delays included the following:

- The medical staff was forced to write discharge instructions and notes on paper.
- The electronic lists of instructions and of medications were not available for the patients being discharged.
- Patients being discharged could not be given follow-up appointments at the time of discharge. The appointments had to be made later and the patient notified by phone.
- There were delays in obtaining discharge medications and patients remained on the wards longer than would normally be required.
- The nurses administered medications to the patients and used the paper MAR to record the administration events. Initial medication passes were interrupted and delayed until the paper copies of the Medication Administration Record (MAR) could be printed.

The use of the paper MAR continued well after the system came back up at around 4 pm. This occurred because there was a delay in the automated updating of all the medications with new orders and changes. Until both Pharmacy and Nursing can verify that the electronic lists have been updated and are accurate, the electronic MAR cannot be used. One inpatient did not meet inpatient criteria but could not be transferred to the nursing home since adequate records were not available. The patient stayed an extra 4 days and required an additional nurse to stay in his room as a sitter until he could be transferred.

Disruption Impact on Outpatient Care

Outpatient activities were impacted within a few minutes after the outage. Although most clinics did not have scheduled patients until 8:00 am, many providers who were beginning to prepare for clinic were affected almost immediately. Consent forms that had been done previously for scheduled surgery and for other procedures were not available since these are all done electronically. The providers with patient appointments early in the morning had no medical records to use for these patients. For many of the patients, a medication list was available on paper but the paper health summary backups had not yet been printed. We began to instruct the users to print the paper health summaries for use in the clinics and on the wards just after 8:00 am. These were distributed as quickly as possible but for patients with appointments at 8:00 am to 9:00 am, very few of these summaries were available in time to provide the needed information to the provider while seeing the patient.

Disruption Impact on Pharmacy

The pharmacy quickly became overloaded with prescriptions that they were attempting to fill for patients. The labeling equipment and automated dispensing equipment, both linked to VistA, were unavailable. The pharmacy began to ask patients if they could wait to have the prescriptions mailed. This problem was made more difficult by the fact that Monday, September 3, 2007, was Labor Day and the next transmission to the Centralized Mail Out Pharmacy (CMOP) would be on Tuesday, September 4, 2007. In addition, the transmission to the CMOP for August 31, 2007 was scheduled for 8:00 am. This also caused a delay in patients receiving medications. The prescription entries completed on August 30, 2007 by the pharmacy were not received at the CMOP for fulfillment until September 4, 2007.

Other Impacts Resulting From the Disruption

The local health summaries for patients were printed in all clinic areas and on the wards which essentially created a temporary patient record. After 2 hours, most users began to record their documentation on paper. For example:

- Paper order forms were distributed and orders were being faxed to Pharmacy and Radiology for inpatients and outpatients.
- Paper prescriptions were written for outpatients.
- Laboratory orders were written on paper and patients sent to the lab with paper copies of orders.
- Multiple patients who had planned CT scans and who needed a measure of kidney function prior to the procedures had to have their blood redrawn since the prior results were not available.
- Consent forms were done on paper.
- Vital signs and screenings for depression, post-traumatic stress disorder (PTSD) and other interventions were recorded on paper.
- The cardiologists could not read any of the EKGs that had been done prior to the failure since these had not been printed and are usually reviewed and interpreted online.
- Surgeons could not enter their operative notes in to the surgery package. Consults could neither be ordered or responded to or even updated.

- Appointments could not be made and, if a patient canceled, there was no way to identify other patients to fill those slots.

Although the paper health summaries were available for patients with scheduled appointments, there were no records at all available for patients who came to Urgent Care or to the Sacramento ER or walk-in patients at any of the clinics.

Prior Computer Failures

Although we have had brief periods of scheduled and occasionally unscheduled computer failure in the past, many of these were isolated to one site or one building and none lasted as long as the disruption experienced on August 31, 2007. Our contingency plans had been implemented successfully as drills during many of these periods. During prior outages, the local IT staff had always been very forthcoming with information on the progress of the failure and estimated length even in the face of minimal or no knowledge of the cause. To my knowledge, this was absent during the most recent outage.

Disruption Recovery

Once the disruption was resolved, a tremendous amount of work was undertaken to restore the integrity of the electronic record. Laboratory and pharmacy staff worked late that Friday night and over the weekend to update the results and orders in the electronic record and to enter all the new orders and outpatient prescriptions. Complete recovery in the pharmacy took over a week. Administrative staff worked for over 2 weeks to complete the checkouts on all the patients who were seen that day. However, entering checkout data on all these patients many days after the fact is potentially inaccurate. Many providers have gone back into CPRS and tried to reconstruct notes that summarize the paper notes that they wrote in order to mitigate the risk of missing information.

This work to recover the integrity of the medical record will continue for many months since so much information was recorded on paper that day. When you consider that hundreds of screening exams for PTSD, depression, alcohol use, and smoking, and entry of educational interventions, records of outside results, discharge instructions and assessments are all now on paper and are not in a format that is easily found in the electronic record, the burden of this one failure will persist for a long time. This adds an additional load for the staff to have to pull up the paper records from that day and presents a risk that some important facts or results collected on that day will be missed at some point in the future. For example, consent forms done that day for future procedures will not be in the same location as our usual consent forms since these were done on paper and scanned into the record during recovery.

In summary, there were severe impacts to patient care, timeliness of care and the integrity of the medical record due to the disruption and these affects will persist for some period of time into the future. Mr. Chairman, this concludes my statement.

POST HEARING QUESTIONS AND RESPONSES FOR THE RECORD

Committee on Veterans' Affairs
Washington, DC.
October 3, 2007

Honorable Gordon Mansfield
Acting Secretary
U.S. Department of Veterans Affairs
810 Vermont Ave., NW
Washington, DC 20420

Dear Mr. Mansfield:

In reference to our Full Committee hearing *VA IT Reorganization: How Far Has VA Come?* on September 26, 2007, I would appreciate it if you could answer the enclosed hearing questions by the close of business on November 14, 2007.

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 by fax to Debbie Smith at 202–225–2034. If you have any questions, please call 202–225–9756.

Sincerely,

BOB FILNER
Chairman

DT:ds

Questions for the Record
The Honorable Bob Filner, Chairman
House Committee on Veterans' Affairs
September 26, 2007

VA IT Reorganization: How Far Has VA Come?

In the September 26, 2007, report of Valerie Melvin, Director of Human Capital and Management Information Systems Issues at GAO ("GAO Statement"), GAO stated:

> *As part of the new organizational structure, the department identified 25 offices whose leaders will report to the five deputy assistant secretaries and are responsible for carrying out the new management processes in daily operation. However, as of early September 2007, seven of the leadership positions for these 25 offices were vacant, and four were filled in and acting capacity.*

Question 1: Please identify for each of those 25 offices:

a. the name of the office and its function;
b. the date on which the leadership position in each office was filled and the person filling the position;
c. for offices for which the leadership position is filled on an acting basis, the date on which the leadership position in each office was filled on an acting basis, the person filling the position, and the date by which the position will be permanently filled; and,
d. for offices for which the leadership position is vacant, the date by which the position will be permanently filled.

Response:

Office Name/Function	Permanent Person & Date Position Filled	Acting Person & Date	Date Vacant Position Projected to be Filled
1. Privacy and Records Management—Integrates privacy considerations into the way the Department of Veterans Affairs (VA) uses technologies and handles information. Oversees compliance with Privacy Act of 1974, Freedom of Information Act, Health Insurance Portability and Accountability Act (HIPAA), Electronic Communications Privacy Act, Office of Management and Budget (OMB) Circular A–130, and Government Paperwork Reduction Act. Completes privacy impact assessments on new programs.	Sally Wallace, 10/1/2006	N/A	N/A
2. Cyber Security—Sets policy and oversees implementation and operation of VA's information technology (IT) security program. Providing information security protection commensurate with risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of: (1) Information collected or maintained by or on behalf of VA, (2) Information systems used or operated by VA or by a contractor of VA or other organization on behalf of VA.	Jaren Doherty, 2/4/2008		
3. Education and Training—Oversees VA-wide cyber security training, education and awareness program, as well as VA annual information security conference. Manages VA's internal information security working group. Ensures VA policies comply with regulatory requirements and legislated mandates.	Terri Cinnamon, 11/8/2007	N/A	

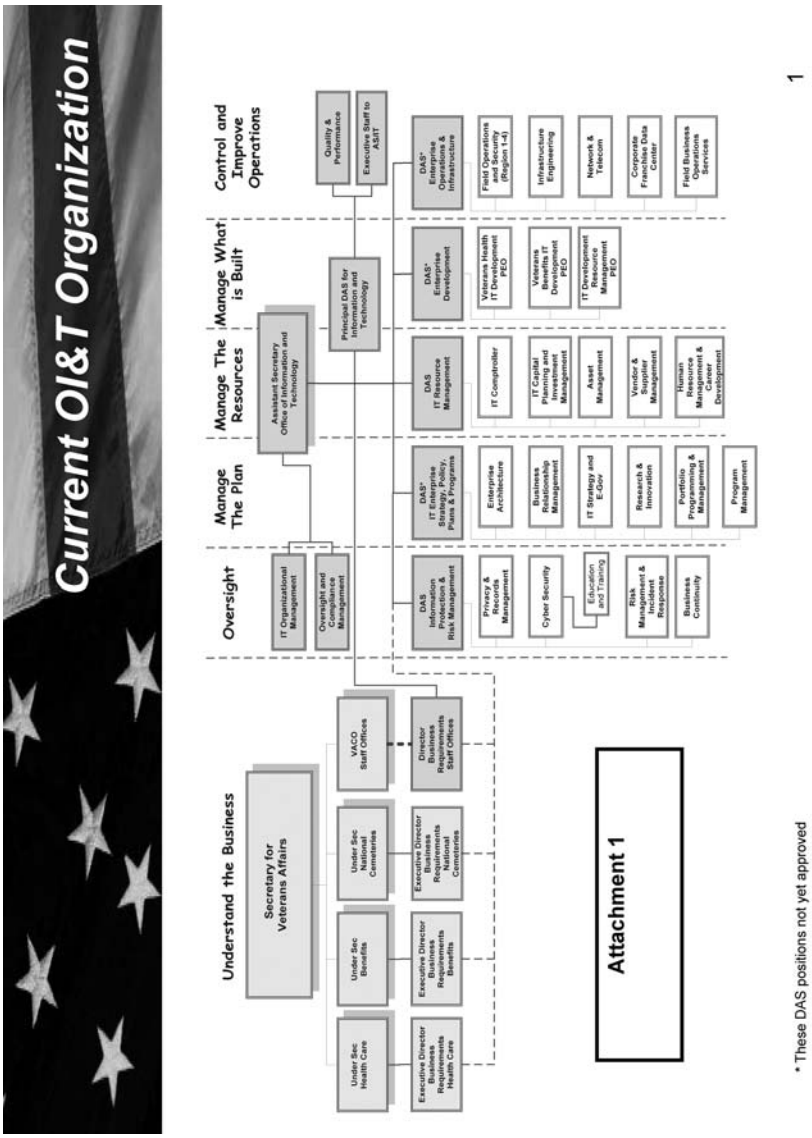
Office Name/Function	Permanent Person & Date Position Filled	Acting Person & Date	Date Vacant Position Projected to be Filled
4. Risk Management & Incident Response—Develops cost effective strategies for IT risk management (encompassing IT risk, business continuity management and information security management) for data processing environments under the control of the Chief Information Officer (CIO).	Katherine Maginnis, 4/29/2007	N/A	N/A
5. Business Continuity—Manage processes to identify potential threats to business continuity and develops capability to effectively safeguards interest of its key stakeholders.	Andres Lopez, 10/29/2007	N/A	N/A
6. Enterprise Architecture—Develops an enterprise-wide technical architecture that enables the business activities of VA and facilitates the adaptation of technology to meet the changing business needs.	Scott Cragg, 8/22/2004	N/A	N/A
7. Business Relationship Management—Negotiates business requirements on behalf of the administrations with IT solution providers.	Vacant	Ross Smith, 11/11/07	3/31/2008
8. IT Strategy and E-Gov—Leads ad-hoc teams of information architects, in developing, best practices and standards that will integrate paper processes into electronic systems.	Loise Russell, 4/24/2007	N/A	N/A
9. Research and Innovation—Identifies new technologies that provide benefit to VA and enables improved level of service to veterans.	Vacant	N/A	12/1/2008
10. Portfolio Programming and Management—Assist in developing IT project management plans, and investment protocols, to meet legislative requirements of Federal capital asset programs	Vacant	Tim Weigel, 11/11/2007	3/31/2008
11. Program Management—Oversees integrated IT management process, reviews milestones and assures IT projects are on schedule, within budget and meet performance criteria.	Vacant	Michael Osband, 1/28/2008	3/31/2008
12. Information Technology Comptroller—Manages financial processes of the Office of Information and Technology (OIT) including budget formulation and execution, cost accounting, cost recovery, cost allocations, charge-back models, and revenue accounting.	Len Bourget, 2/18/2007	N/A	N/A
13. Human Resource Career Development—Aligns OIT human resource management with VA's Office of Human Resource and Administration (HRA) and the Office of Personnel Management.	Vacant	Thomas Barritt	2/28/2008
14. IT Capital Planning and Investment Management—Plans and controls IT budgets; and evaluates financial performance.	Vacant	Karen Kemmet, 7/1/2007	3/17/2008
15. Asset Management—Provides users with hardware and software needed to do their jobs in the most cost effective manner.	Gary Shaffer, 12/9/2007	N/A	N/A
16. Vendor and Supplier Management—Develops, implements, and manages sourcing strategies to improve the process of negotiating and managing IT contracts and evaluating vendor performance.	Vacant	N/A	12/1/2008
17. Veterans Health IT Development Program Executive Office (PEO)—Manages IT development activities in support of the Veterans Heath Administration (VHA).	Vacant	Jackie Gill, 9/15/2007	3/31/2008
18. Veterans Benefits IT Development PEO—Manages IT development activities in support of the Veterans Benefit Administration (VBA).	Richard Culp, 4/1/2007		
19. IT Development Resource Management PEO—Manages development, integration and implementation of new enterprise applications within resource management systems portfolio.	Joseph Bond, 4/1/2007		

Office Name/Function	Permanent Person & Date Position Filled	Acting Person & Date	Date Vacant Position Projected to be Filled
20. Memorial Affairs IT Development PEO—Manages the development, integration and implementation of new enterprise applications within the National Cemetery Administration (NCA).	Dan Pate, 9/30/2007	N/A	N/A
21. Field Operations and Security—Manages day-to-day IT operations, data centers, IT services and IT security across 4 geographic regions.	Raymond Sullivan, 10/29/2006	N/A	N/A
22. Infrastructure Engineering—Tests, evaluates and certifies software and hardware prior to deployment. Responsible for change management, systems engineering, configuration management, release management, production control and maintenance.	Charles DeSanno, 1/2/2007	N/A	N/A
23. Corporate Franchise Data Center—Provides IT services to VA medical centers, regional offices, national cemeteries, and other VA and non-VA organizations.	Vacant	John Rucker, 8/1/2007	3/17/2008
24. Field Business Operations and Services—Controls and improves the processes, services and outcomes relative to end user support, network services and security services.	Gary Twedt, 10/29/2006	N/A	N/A
25. Network and Telecom—Providing telecommunication systems to support VA requirements.	David Cheplick, 7/22/2007	N/A	N/A

Question 1(e): In addition, please provide organization charts showing the reporting relationships of the 25 offices to the five deputy assistant secretaries.

Response: See Attachment 1 on next page.

Attachment 1



Question 2: Please provide a timeline for completion separately for each of the following three:

Question 2(a): The 36 new processes of the IT management processes, including the 9 of the 36 that the VA began implementing in March 2007.

Response: The 36 core IT business processes are undergoing process improvement, ultimately resulting in the development of a series of improved, standardized processes across all business lines. These improved processes will be developed by teams of experts, documented, and disseminated across VA to ensure that they are repeatable by all VA IT entities. The availability of standard operating procedures will not only ensure consistency from site to site, but will also prevent duplication

of effort in developing them. VA process maturity levels will evolve and improve over time based on continuous refinement and process improvement.

The timeline for the 36 core IT management processes calls for implementation by July 2008. We have completed process redesign pilot programs for two: (1) risk management and (2) solution test and acceptance. In addition, Process Manuals exist for 27 of the processes, either in draft or final version. Key meetings have been held for 20 of the processes, with approximately 8 more planned for the week of February 11, 2008. The attached spreadsheet provides the details for each of the 36 processes.

The approach and schedule for process implementation has been revised, based upon lessons learned from the pilot programs and current implementation experiences. We are streamlining the process improvement approach in order to meet the July 2008 timeframe.

Attachment 2 provides a listing of all 36 processes and the status of each.

Attachment 2

Status of 36 New IT Management Processes
3/13/2008

Process	Process Manual Complete	Status of Process	
		Procedure(s) or Guidance	
		In Review	Complete
Capital Planning & Investment Control	✔		✔
Project Management	draft	✔	
Service Level Management	draft	✔	
Architecture Management			
Customer Satisfaction Management			
Data and Storage Management			
IT Research & Innovation			
IT Strategy	draft		
Knowledge Management			
Service Marketing and Sales			
Stakeholder Requirements Mgmt			
Asset Management	✔	✔	
Financial Management	draft		
Supplier Relationship Management			
Workforce Management	draft		
Compliance Management	✔		✔
Change Management	✔	✔	
Configuration Management	✔	✔	
Facility Management	draft		
Release Management	✔	✔	
Service Execution	draft		
Availability Management	draft		
Capacity Management	draft		
Event Management	draft		

Process	Process Manual Complete	Status of Process	
		Procedure(s) or Guidance	
		In Review	Complete
Incident Management	draft		
Problem Management	draft		
Service Pricing & Contract Admin	draft		
User Contact Management	draft		
Solution Test and Acceptance	✔		
Solution Analysis and Design	✔		
Solution Build	✔		
Solution Requirements	✔		
Risk Management	✔		
IT Service Continuity Management	draft	✔	
Security Management		✔	
IT Management System Framework	✔		

Question 2(b): The 20 out of the 22 information security-related recommendations made by the inspector general in 2006, including any updates on the status of the 2 of 22 implemented. The status and targeted completion date of the 17 FISMA related findings made by the VA Office of Inspector General recommendations in its annual FISMA report for fiscal year 2005, issued in September 2006.

Response: The 22 recommendations related to information security made by the Inspector General in 2006 consist of:

- The 17 recommendations in the *Office of Inspector General (OIG) Fiscal Year (FY) 2005 Audit of VA Information Security Program* (report number 05–00055–216 dated September 20, 2006); and
- The five recommendations from the OIG Report: *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Americans* (report number 06–02238–163 dated July 11, 2006).
- In addition to the 22 recommendations, 13 recommendations were made as a result of the OIG's FY 2006 audit work and are published in the OIG's *FY 2006 Audit of VA's Information Security Program* (report number 06–00035–222) dated September 28, 2007.

Recommendations number 6 and 12 from the *OIG FY 2005 Audit of VA Information Security Program* (report number 05–00055–216 dated September 20, 2006) have been closed out by the OIG. All of the recommendations and status are listed below:

Target completion dates for corrective action have been included below, where available. Data Security—Assessment and Strengthening of Controls Program (DS–ASC) personnel will be working with personnel responsible for implementation of corrective action to obtain target completion dates for all OIG recommendations shown below.

Recommendations from FY 2005 Audit of VA Information Security Program, Report Number 05–00055–216, September 20, 2006

Recommendation 1. Implement a centralized IT management approach; apply appropriate resources; establish, clarify, and modify IT policies and procedures pursuant to organizational changes; and implement and enforce security controls.

Status: Corrective Action Still in Process.

All IT personnel and the entire IT budget have been placed under the control of the Assistant Secretary for OI&T, who serves as the VA CIO. Over the past year, the CIO has issued policies, procedures, and directives implementing this new, centralized management concept to include VA Directive 6500, *Information Security Program* and its accompanying handbook, VA Handbook 6500. Several other policies

providing guidance regarding implementation of IT security controls are either in draft or in concurrence.

In addition, the CIO is centrally managing implementation, enforcement, and remediation of IT security controls throughout VA via the data security assessment and strengthening of controls (DS–ASC) program and has established the Office of IT Oversight and Compliance (ITOC) which consolidates existing IT security activities into one office to assist in centralizing enforcement of IT security controls.

Recommendation 2. Develop and implement solutions for the establishment of a patch management program.

Status: Corrective Action Still in Process. The enterprise framework (EF) will provide centralized IT infrastructure management by asset management and software delivery (inventory and configuration) and interface with the patch management process (portal and policy compliance). The current project status is as follows:

- Completed proof of concept with the integration of two Veteran's Integrated Service Networks (VISN). The second quarter of FY 2007 focused on developing configuration and process baselines. This was followed by deploying and integrating three additional VISNs, to form a centrally managed Region, during the third quarter of FY 2007 through the third quarter of FY 2008. This will be repeated in Regions 2, 3, and 4.
- VA has deployed a vulnerability and patch remediation solution (i.e., Harris STAT Guardian and previously Citadel Hercules) that the field has been using since 2003 to scan systems and remediate deficiencies. VA has over 300 dedicated Harris STAT servers providing scan and automated patch capabilities across the VA IT enterprise today. This does not include other patch remediation tools that have been deployed locally such as systems management server and update expert. VA has spent approximately $15M since 2003 on an enterprise-wide vulnerability and patch remediation solution. The long term solution is to leverage the EF to provide this capability.

In addition, other completed actions to implement a patch management program for the VA enterprise are as follows:

1. Current practices have been gathered (completion date August 2007).
2. Patch management working group charter, process, and list of deliverables have been developed (completion date October 2007).
3. Patch management working group and working group lead have been identified (completion date December 2007).
4. Memorandum issued, titled *Enterprise Patch Management Requirements,* detailing VA's patch management program's roles and responsibilities, key personnel contact information, and standard operating procedures for field implementation (completion date December 2007).

Other actions that still need to be accomplished include:

1. Review of all current patch management practices across VA, target date for completion is late March 2008.
2. Development of VA patch management policy, target date for completion is May 2008.
3. Development of a patch management program to support configuration management procedures, target date for completion is November 2008.
4. Implementation of the patch management program and training plans enterprise wide, target date for completion is September 2009.

Recommendation 3: Identify and implement solutions for resolving access control vulnerabilities, ensure segregation of duties, remind all sites to confirm virus protection fields are updated prior to authorizing connection to their networks, and resolve all self-reported access control weaknesses.

Status: Corrective Action Still in Process. VA IT Directive 06–1, *Data Security: Assessment and Strengthening of Controls,* dated May 24, 2006, established a program to remediate the IT security controls material weakness. As a result the DS–ASC plan was developed to address deficiencies. The target date for resolution of these deficiencies is third quarter of FY 2008.

Recommendation 4: Review and update all applicable position descriptions to better describe sensitivity ratings, better document employee personnel records and contractor files to include signed "Rules of Behavior" instructions, annual privacy and HIPAA training certifications, and position sensitivity level designations.

Status: Corrective Action Still in Process.

With issuance of the Secretaries June 28, 2006 memorandum, the Assistant Secretary for OI&T now has complete responsibility and authority for information security policies, procedures, and practices to include risk and sensitivity levels of employee position descriptions.

Position descriptions and their corresponding sensitivity designations are being reviewed for consistency VA wide. Based on the results of these reviews, self certifications from VA's organizational components indicate that VA has requested approximately 95 percent of its required background investigations.

In addition, a VA national *Rules of Behavior* document is included in an appendix to the recently published VA Handbook 6500 and will be signed by personnel with access to VA information systems and placed in the appropriate file. VA reported to OMB that 95 percent of its employees completed FY 2007 cyber security awareness training.

Recommendation 5: Timely request the appropriate levels of background investigations on all applicable VA employees and contractors. Additionally, monitor and ensure timely requests for reinvestigations on all applicable employees and contractors.

Status: Corrective Action Still in Process.

Department wide, implementation of this recommendation is approximately 95 percent complete. The Department is awaiting input from the remaining organizations to certify that all required background investigations have been initiated.

In December 2006, the Office of Security & Law Enforcement within the former Office of Policy, Planning and Preparedness published a notice providing guidance for requesting the appropriate level of backgrounds for contractors and the proper procedures for processing these requests. Additionally, VA Directive 0710 was revised and has been placed in the concurrence process. The amended Directive 0710 provides more detailed guidance for processing employee and contractor background investigations. VA Handbook 0710 is currently being revised and is planned to be completed within the next several months.

The Security and Investigations Center (SIC) has developed and is using a computer tracking system that will automatically generate a notice to the SIC staff when an employee or contractors is due a background reinvestigation. This tracking system will ensure that a timely notice is sent to the employee or contractor when reinvestigation packets are due to be completed.

Recommendation 6: Provide our office the results of researching the benefits and costs of deploying intrusion prevention systems (IPS) at all sites.

Status: Closed by the OIG.

Recommendation 7: Continue efforts to strengthen critical infrastructure planning, complete the critical infrastructure protection plan, and ensure infrastructure planning addresses Executive Order 13231, and other information security requirements.

Status: Corrective Action Still in Process.

VA has completed the following critical infrastructure protection actions:

- Security training was provided to the appropriate personnel assigned to the Network and Security Operations Center (NSOC). The new hires will have training this year.
- Encryption software was installed on all laptops by September 2006.
- The Critical Infrastructure Protection (CIP) division is implementing the public key infrastructure (PKI) solution. Over 135,000 PKI certificates have been issued to date.
- VA has a continuity of operations plan (COOP) and comprehensive emergency program plan. OI&T participates in VA's annual master COOP plan test. Primary responsibility for the VA's master COOP plan rests with the Office of Operations, Security, and Preparedness (OSP). VA has issued Directive and Handbook 0320, *Comprehensive Emergency Management Program.* Both are dated March 24, 2005. VA also has an OI&T COOP plan which was posted to VA Intranet in June 2003.
- VA's critical infrastructure protection contingency plan references Homeland Security Presidential Directive—HSPD 7, Homeland Security Act 2002, National Response Plan, and National Incident Management System (NIMS) plus other

historical cyber security requirements. The CIP division is working with the Office of Cyber Security to incorporate the requirements, recommendations and guidelines into the policies and procedures. Target completion date is August 2008.

- The CIP division is installing network intrusion prevention (NIP) devices capable of monitoring and blocking network traffic. The VA NSOC is performing an analysis to see what other locations can benefit from the NIP units. This is an ongoing process where we continuously re-evaluate to ensure the VA has adequate coverage with regards to the NIPS.

Recommendation 8: Collaboratively test ITC COOPs in a joint effort with all tenant groups (VHA, VBA, NCA, and other program offices) to ensure that backup sites will support all mission related operations, and report test results to our office for further review.

Status: Corrective Action Still in Process.

The Corporate Franchise Data Center (CFD), Austin Campus (formerly the Austin Automation Center or AAC) conducts COOP tests annually and has integrated its COOP test with the organizations collocated at its facility. The test includes the following:

1. Verifying the ability of CFD, Philadelphia Information Technology Center (ITC), and Hines ITC staff to recover the CFD Mission Critical and Essential Support systems currently replicated to the Philadelphia and Hines ITCs. Examples of Mission Critical and essential Support systems include applications such as PAID, VETSNET and FMS.
2. Testing the ability of the CFD to use its workspace recovery facility for CFD staff to remotely log onto CFD recovery platforms using the OneVA virtual private network (VPN).
3. Testing CFD, Philadelphia Insurance, and Veterans Benefits Administration (VBA) Benefits Delivery Network (BDN) end-to-end transmission of files between the Hines ITC, Philadelphia ITC, Financial Services Center (FSC) Waco facility, and Treasury's Hyattsville Processing Facility.
4. Testing Beneficiary Identification and Records Locator System (BIRLS) functionality between the Hines and Philadelphia ITCs.

The last disaster recovery (DR) exercise for the CFD, Austin Campus was conducted in August 2007; the next exercise is scheduled for August 2008. Mission critical and essential support applications are tested with resident organization input during the annual DR exercise. Table top tests were performed on routine applications in 2007.

The Philadelphia ITC established an agreement between the ITC, Philadelphia Regional Office and Insurance Center (ROIC), and the Philadelphia VA Medical Center (VAMC) that established a command post at the VAMC for key ITC and ROIC personnel for disaster recovery purposes. The Philadelphia ITC conducted full DR tests for the VBA Web applications and the Insurance Payment System in April/May 2007. A BDN disaster recovery test by Hines and Philadelphia staff was performed in Philadelphia July 9–12, 2007. A joint exercise including tenants is planned in 2008; however, this will be a simulated or desktop exercise and not a full DR test. The next VBA web application disaster recovery test is scheduled for the May–June 2008 timeframe at Hines Information Technology Center. We also plan to conduct the Insurance Payment System disaster recovery test during this same timeframe.

The Hines ITC maintains a comprehensive DR plan for the legacy Benefits Delivery Network (BDN). The disaster recovery exercise in July 2007 successfully demonstrated that the Bull and IBM BDN disaster recovery infrastructure at the Philadelphia ITC is capable of executing the BDN online and batch processing in the event of a real disaster. This plan is exercised annually in the summer months. The Hines ITC conducted a joint table-top exercise in December 2007.

Recommendation 9: Address all self-reported deficiencies identified as the result of completed C&A and related review work.

Status: Corrective Action Still in Process.

In May 2006, the CIO issued VA IT Directive 06–1, *Data Security: Assessment and Strengthening of Controls.* This directive established a program to remediate IT security controls deficiencies. From this DS–ASC plan was developed which addresses deficiencies resulting from completed certification and accreditation (C&A) work,

details of which are contained in the plans of actions and milestones (POA&M) section of the security management and reporting tool (SMART) database.

The Office of Oversight and Compliance has been established to ensure continuity and followthrough on remediation of these deficiencies.

Recommendation 10: Determine the extent to which uncertified Internet gateways continue to exist, and take actions to upgrade and terminate external connections susceptible to inappropriate access.

Status: Corrective Action Still in Process.

NCA shut down its Internet gateway on June 20, 2006.

VBA shut down its Internet gateway a year ago. VBA continue to maintain a private T1 connection to benefits delivery discharge (BDD) centers at two military facilities in Korea and Germany. VBA routes no other data traffic to them, and they are getting ready to ship preconfigured firewalls to these centers. The T1 connections will be removed within the next 3 months and the traffic will route through a virtual private network (VPN) when the firewalls are installed.

VHA's VISN 20, 21, and 22 have migrated its traffic to the enterprise cyber security infrastructure program (ECSIP) and have shut down their external connections; however, VHA has identified additional external business connections that require business partner gateway (BPG) VPN connections. These connections are documented, justified, and submitted to the enterprise security cyber control board (ESCCB) for approval.

The Environmental Protection Agency (EPA) connection moved to the ECSIP gateway and the moving of the remaining connections is contingent on ESCCB approval. In March 2007, the AAC moved all of it's existing site-to-site VPN connections to the AAC's Internet firewall, and then moved the AAC's Internet firewall's and franchise firewall's internal interfaces from the internal gateway to the VA wide area network (WAN). This was necessary to complete the process of moving site-to-site VPNs and Internet facing web servers to the VA WAN for Internet access, thus allowing the shutdown of the supporting Internet service provider. ESCCB approval is pending for a plan to migrate the Internet facing web servers as the next step in the process.

Significant progress is being made with migrating Corporate Franchise Data Center (CFD) (formerly Austin Automation Center) remaining customers off of the CFD Internet gateway. DoD traffic will be migrated by the end of February 2008 and all other customers such as Home TeleHealth (HTH), Workman's Compensation, and the National Archives and Records Administration (NARA) will be completely migrated by June 30th, 2008.

Recommendation 11: Improve configuration management practices by identifying, replacing, or justifying the continuance of older operating systems that are vulnerable to security breaches.

Status: Corrective Action Still in Process.

VA has been upgrading its computers to the Microsoft Windows XP operating system and also has been upgrading peripheral devices, as necessary.

All VBA workstations are operating under Windows 2000, and all VBA servers are operating under Windows 2003. Implementation plans are underway for workstation upgrades to Windows XP. However, the conversion to newer operating systems for VBA platforms is dependent upon upgrading the applications systems code to use the newer operating systems capabilities. The applications upgrade has been estimated at approximately $2 million and will take approximately 2 years to complete. Application upgrading will begin and the conversion to a newer operating system can be accomplished at the end of this upgrade process. VA is currently working to develop requests for waivers for these applications until the application upgrade can be accomplished.

In VHA most desktop systems or IT servers use the latest operating system, Windows XP. The exceptions to this rule includes specialized equipment incorporating an operating system such as three V–Tel systems in VISN 17 using Windows 98 and one telephone switch in VISN 19 using Windows 98 as well as medical devices. The V–Tel systems and telephone switch are connected via a virtual local area network (VLAN) that provides isolation from the facility LAN which is being replaced. All medical equipment, regardless of the operating system, is required by VHA policy to be connected to facility networks using the VA isolation architecture. Some medical systems cannot be upgraded.

Configuration management has been addressed in the recently published VA Handbook 6500. In addition, a plan to address configuration management defi-

ciencies was completed in August 2007. Minimum configuration settings for information technology products were established in September 2007 and submitted in October 2007 to the configuration management technical working group (CM/TWG) for finalization and approval in conjunction with enterprise change and configuration management processes. In September 2007 VA decided on replacement requirements for personal equipment.

Field security operations are in the process of defining a process to standardize operating systems and applications. Processes are also being developed for monitoring system changes and their impacts. Target date for completion is late March 2008 with final completion dependent on the CM/TWG and the testing/procurement of an enterprise management framework (EMF) toolset to support these processes. The CM/TWG has a target completion date of September 30, 2008, to develop the needed change control procedures, and the EMF project has a target completion date of FY 2009, with pilot testing in the last quarter of FY 2008.

Recommendation 12: Complete actions to relocate and consolidate VACO's data Center.

Status: Closed by the OIG.

Recommendation 13: Develop and implement VA-wide application program/operating system change control procedures to ensure consistent documentation and authorization practices are deployed at all facilities.

Status: Corrective Action Still in Process.

Change control, as a required security control defined in the National Institute of Standards and Technology (NIST) Special Publication 800–53, is included in the recently published VA 6500 Handbook. A new technical oversight Committee has been established, chaired by the Office of Development, and will review the need for specific and separate change control policy beyond the scope of VA Handbook 6500.

Additionally, the IT regional data processing change management process is establishing integrated change control and ultimately a full change management process. The current outcome is a change management process with an interim definition established in a January 29, 2007 memorandum—*Regional Data Processing Information Technology Change Management Interim Process*—which focuses on change requests that may impact the infrastructure or operating environment of the regional data processing. The work group will establish a full change management process and ultimately configuration management. This workgroup and processes are linked with VBA's architecture change and review board, AAC's change management process and change control board, and ESCCB. This work group will look at incorporating other change control processes such as those used by VA developers. There is a process definition technical work group that will define the VA process for change management.

Related actions that have been completed regarding implementation of change controls throughout the VA enterprise include:

1. Current change control practices have been gathered, completion date August 2007.
2. Change control working group charter, process, and list of deliverables have been developed, completion date October 2007.
3. Change control working group and working group lead has been identified, completion date December 2007.

Related actions that still need to be accomplished regarding change controls include:

1. Review all current practices across VA focusing on the impact to operating systems including security, target date for completion is late March 2008.
2. Develop change control policy, target date for completion is May 2008.
3. Develop change control procedures, target date for completion is November 2008.
4. Implement change controls and training plans VA wide, target date for completion is September 2009.

Recommendation 14: Strengthen physical access controls to correct previously reported physical access control deficiencies, develop consistent standardized physical access control requirements, policies, and guidelines throughout VA.

Status: Corrective Action Still in Process.

The OSP has revised VA Directive and Handbook 0730, including Appendix B, *Physical Security Requirements and Options.* Along with other major changes, the revised 0730 document contains updated requirements for the physical access of protect IT spaces, such as computer rooms and telecommunication/data connections. This directive is currently pending departmental concurrence. After concurrence is received, in accordance with title 38 section 901 it must then be submitted to the Department of Justice for review prior to publication. The Office of Operations, Security and Preparedness anticipates it may not be until the end of FY 2008 before the revised VA Directive and Handbook 0730 Directive and Handbook are released.

Physical and environmental controls have been addressed nationally in the recently published VA Handbook 6500. Resolution of physical access control deficiencies is an iterative process. VA IT Directive 06–1, *Data Security—Assessment and Strengthening of Controls,* dated May 24, 2006, established a program to remediate the IT security controls material weakness. As a result the DS–ASC plan was developed to address the physical access control deficiencies mentioned above. Target date for remediation of these deficiencies is the third quarter of FY 2008.

The Office of Information and Technology Office of Oversight and Compliance has been established to ensure continuity and followthrough on remediation of physical access control deficiencies. In order to highlight the necessary physical security requirements, the Office of Information and Technology Oversight and Compliance (ITOC) worked closely with representatives from the Office of Operations, Security and Preparedness to develop an Information Physical Security (IP) checklist to be utilized by ITOC during assessments of VA facilities. The IP checklist has been added to the assessment protocols. The initial prototype was tested at a number of VA facilities and was well received by Facility Directors, CIOs, Information Security Officers, Chiefs of Police, and others. An early observation indicates it will prove invaluable to direct attention to physical access issues. The ITOC assessment teams are also continuing to stress the applicable security controls from the NIST 800–53 protocols during the assessments.

An Information Memorandum, to be jointly issued by the Assistant Secretary for Operations, Security and Preparedness and the Assistant Secretary for Information and Technology, is being prepared. This joint memorandum will form the basis of a physical security awareness campaign. This memorandum is expected to be released sometime in mid-FY 2008.

Recommendation 15: Reduce wireless security vulnerabilities by ensuring sites have an effective and up-to-date methodology to protect against the interception of wireless signals and accessing the network. Additionally, ensure the wireless network is segmented and protected from the wired network.

Status: Corrective Action Still in Process.

Wireless laptops on VA networks are protected and separated from the wireless network by AirFortress. Methods used to protect the interception of wireless signals and accessing the network are included in VA's *Wireless and Handheld Device Security Guideline, Version 3.2,* dated August 15, 2005.

VHA and VBA have installed AirFortress wireless security gateway to secure their wireless LAN systems. All wireless data traffic is routed through the AirFortress wireless security gateway before it is transmitted on VA network. The AirFortress wireless security gateway not only provides encryption of data between the wireless client and the security gateway, it also provides firewall functionality and limits access to VA network to only authorized devices and users. Since firewall functionality has already been provided as part of the AirFortress solution there is no need to install an additional firewall between AirFortress and VA network.

VA recognizes that any secure wireless LAN system will include a wired/wireless network border gateway security device that will enforce an access control policy between the wired and wireless network thereby limiting access to only authorized users on authorized ports, all features of a firewall.

However, additional work needs to be done in the wireless area. Blackberries and PalmPilots connecting to the network are not encrypted. Encryption for these devices is being piloted. In addition, the NSOC is establishing a wireless assessment program that will identify and assist the field with remediation of wireless security vulnerabilities.

Recommendation 16: Identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.

Status: Corrective Action Still in Process.

VA has taken several actions toward the protection of sensitive information. By September 15, 2006 the VA encrypted over 15,000 laptops. Simultaneously, VA developed and implemented procedures to ensure that all laptops have applied updated security policies and removed all sensitive information that was not authorized to be stored on the devices. This procedure will continue to occur throughout the Department routinely and is one measure VA has undertaken to protect information.

VA has begun deploying technology to ensure information is protected and is identifying and leveraging existing technologies that will contribute to protecting VA information. These technologies and the status of their deployments are shown below:

- *Sanctuary* port security and device control technology. *Sanctuary* has been deployed and is operational in Region 4 (Northeastern United States). *Sanctuary* is actively restricting the use of non-VA approved universal serial bus devices on VA computers. The technical documentation, architecture design, server configuration, and project documentation created during Region 4 deployment are being leveraged by the rest of the enterprise as they begin deployment of the technology. Region 3 (Southern/near Midwestern United States) will be the next region to deploy *Sanctuary* and is in the process of procuring hardware to support its implementation. Subsequently, Region 1 (Western United States), Region 2 (Southwestern/far Midwestern United States), the Corporate Franchise Data Center (Austin, Texas), VBA, and NCA will deploy.
- *Microsoft Rights Management Services (RMS)* technology to safeguard digital information from unauthorized use. VA completed the deployment of over 157,000 *RMS* clients across the enterprise in FY 2007. VA procured robust hardware to support the operations of *RMS* for the enterprise, thus enabling VA to use the current hardware for the infrastructure for the *RMS* continuity of operations. VA has begun to test the external provisioning component for *RMS* which will extend the *RMS* functionality of protecting emails and documents to VA business partners. Without the external provisioning component, VA business partners, such as the Department of Justice, cannot read email messages that are sent with *RMS* security controls applied.
- *Attachmate* host integration and secure network transmission technology. In 2007 VA conducted pilot testing of *Attachmate* technology across all of VA's Regions. The pilot included the installation and testing of the terminal emulator client in unencrypted mode and then encrypted mode. This technology will be able to encrypt information sent across VA network from applications such as VistA (veterans health information systems and technology architecture), CPRS (computerized patient record system), and IFCAP/ETA (integrated funds distribution, control point accounting and procurement/enhanced time and attendance). VA has developed the various configurations depending on how the product will be used to include the corresponding technical documentation. The installation package and the technical documentation will be posted to a share point and made available for sites to acquire this information and the file. Region 4 will be the first to deploy the client in an encrypted mode throughout their region.
- *Cisco* and *BigFix* secure remote access technology. The secure remote access project, also known as the remote enterprise security compliance update environment (RESCUE), proof of concept was successfully completed in mid-October 2007. The RESCUE solution consists of *Cisco* technology for enforcement and network access control and *BigFix* for remediation of non-compliant devices. Recently, VA NSOC installed a portion of the hardware to support RESCUE in the Reston gateway. In January 2008 a small user group test was conducted out of the Reston gateway. Simultaneously, RESCUE hardware and software will be installed in the remaining gateways by February 2008. The virtual private network (VPN) user-base will be migrated to the RESCUE solution by June 2008.

Recommendation 17: Conduct validation tests in conjunction with remediation efforts to ensure all information and data retained in the SMART database is accurate, complete, and reliable.

Status: Corrective Action Still in Process. ITOC performs validation tests of SMART database as part of their assessments. To date numerous assessments have been conducted by ITOC. ITOC has validated internal processes and procedures in the identification and accuracy of POA&M items and has stressed to the field the need to ensure updated information is incorporated into SMART. The ITOC inspection checklist has been modified to add additional task lines to verify entries in SMART. Target completion date is April 1, 2008.

Recommendations from OIG Report: Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Americans, Report # 06–02238–163, Issued July 11, 2006

Recommendation 1: Establish one clear, concise VA Policy on safeguarding protected Information when stored or not stored in VA automated systems, ensure that the policy is readily accessible to employees, and that employees are held accountable for non-compliance.

Status: Closed by the OIG based on the issuance of VA Handbook 6500, Information Security Program, on September 18, 2007 and meeting with OIG on September 7, 2007.

Recommendation 2: Modify the mandatory Cyber Security and Privacy Awareness training to identify and provide a link to all applicable laws and VA policy.

Status: Corrective Action Completed. Cyber security and privacy awareness training modules have been updated. The privacy awareness training module has been updated and now contains links to applicable laws and VA policy. It has been provided to the OIG for review. The FY 2008 cyber security awareness training was made available on October 1, 2007. All applicable VA policy and Federal laws are linked on the reference page of the online training course. VA is currently working with the OIG to close out this Issue.

Recommendation 3: Ensure that all position descriptions are evaluated and have proper sensitivity level designations that there is consistency nationwide for positions that are similar in nature or have similar access to VA protected information and automated systems, and that all required background checks are completed in a timely manner.

Status: Corrective Action Still in Process.

- New fields have been added to VA payroll system to reflect position risk/sensitivity levels for each VA position and background investigation levels for each employee.
- The revised version of VA Directive 0710, *Personnel Suitability and Security Program,* is still in concurrence. In addition, the accompanying handbook, VA Handbook 0710, is under development by OSP.

VA will ensure that all background investigations are requested, and as appropriate, adjudicated when completed, in the required timeframes and will monitor the status of investigations performed by outside entities. VA cannot ensure background investigations are completed in a timely manner as VA does not conduct background investigations; these are performed by the Office of Personnel Management.

Self-certifications from VA's organizational components indicate that VA has requested approximately 95 percent of its required background investigations.

Recommendation 4: Establish VA-wide policy for contracts for service that requires access to protected information and/or VA automated systems, that ensures contractor personnel are held to the same standards as VA employees, and that information accessed, stored or processed on non-VA automated systems is safeguarded.

Status: Closed out by the OIG based on the issuance of VA 6500 Handbook, *Information Security Program,* dated September 18, 2007.

Recommendation 5: Establish VA policy and procedures that provide clear, consistent for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems, including specific timeframes and responsibilities for reporting within the VA chain-of-command and, where appropriate, to OIG and other law enforcement entities, as well as appropriate notification to individuals whose protected information may be compromised.

Status: Closed by the OIG based on the issuance of VA Handbook 6500, *Information Security Program,* on September 18, 2007 and meeting with OIG on September 7, 2007.

Recommendations from OIG's FY 2006 Audit of VA's Information Security Program, Report Number 06–00035–222, dated September 28, 2007.

Recommendation 1: Provide for the maintenance of appropriate documentation of completed background investigations for employees and contractors.

Status: Corrective Action Still in Process. Documentation of completed background investigations will be maintained for employees and contractors in accordance with VA policies and procedures.

Recommendation 2: Require contractors with access to VA systems to complete cyber security awareness training in accordance with OMB A–130.

Status: Corrective Action Still in Process. Paragraphs 2 and 3f of VA Directive 6500, *Information Security Program,* dated August 4, 2006, requires annual security awareness training for all contractors with access to VA sensitive information and information systems. VA 6500 Handbook, *Information Security Program,* issued on September 18, 2007, also requires that contractors take this training.

In addition, VA has developed standard contract language to be used in all VA contracts regarding protection of VA information and information systems which will incorporate the requirement for contractors to complete annual security awareness training. The contractual language is still undergoing Departmental concurrence. Target date for obtaining concurrence on this contract language is April 2008.

Recommendation 3: Develop and implement a methodology to assess the effectiveness of VA's Intrusion Prevention Systems in protecting VA systems and data from inappropriate access.

Status: Corrective Action Still in Process. VA will implement a method to evaluate the effectiveness of VA's IPS.

Recommendation 4: Develop a comprehensive COOP for OI&T and update and finalize the OI&T appendix within the VA Master COOP to include its essential functions, emergency relocation group, mission critical systems, and vital records in accordance with the Federal Preparedness Circular 65, Federal executive branch Continuity of Operations.

Status: Corrective Action Still in Process. VA has a master COOP and comprehensive emergency program plan. Primary responsibility for VA's master COOP plan rests with the OSP. OI&T is a part of and participates in VA's annual master COOP plan tested.

OI&T has its own COOP plan which was posted to the VA Intranet in June 2003. This plan is contained in OI&T Handbook 0320, *Continuity of Operations, Planning Procedures and Operational Requirements.* The purpose of the OI&T COOP plan is to:

a. Provide command and control of IT assets during emergency situations to ensure continuation of mission-critical and mission-essential operations.
b. Provide a coordinated response and recovery effort to effectively mitigate an emergency or disaster.
c. Ensure the Assistant Secretary for OI&T can perform its mission-critical and mission-essential responsibilities during and after an emergency situation.
d. Ensure the safety and welfare of VA IT staff both during and after an emergency situation.
e. Provide a mechanism for the prompt notification of all VA IT personnel during an emergency situation.
f. Reconstitute, as rapidly as possible, IT systems that are adversely affected due to an emergency or disaster.
g. Develop mitigation strategies that will ensure the survival of VA's critical IT infrastructure.
h. Support regular training and exercises designed to enable personnel to perform assigned emergency management duties.
i. Provide a standardized format for reporting the status of essential IT systems and functions.

This plan applies to all VA IT staff, and contractors, and its mission of supporting VA Central Office (VACO) with IT, information management, record management, cyber security, and telecommunications. The plan addresses emergency preparedness activities to ensure business continuity. Preparedness activities include plans, procedures, readiness measures, and mitigation strategies that enhance VA's ability to respond to and recover from a designated emergency.

OI&T will complete the identification and prioritization of its critical information assets, essential functions, emergency relocation group, mission critical systems, and vital records and will update and finalize its appendix section within the VA master COOP to make it current with the OI&T reorganization.

Recommendation 5: Ensure the C&A work is complete and that the C&A certifications are supported by the work performed.

Status: Corrective Action Still in Process. Certification and accreditation (C&A) work for VA's information systems is complete. Re-accreditation for the vast majority of VA's systems (which were accredited in August 2005) is due to be completed in August 2008.

In 2006, VA contracted with an outside firm to perform an independent validation and verification (IV&V) of its 2005 C&A effort. VA will review the issues and recommendations contained in the contractor's IV&V report, along with the issues identified on pages 11–13 of this audit report, and make the appropriate revisions to VA's C&A policy to ensure that future C&As are performed according to NIST 800–37.

In 2006, VA contracted with an outside firm to perform an independent validation and verification (IV&V) of its 2005 C&A effort. VA has reviewed the issues and recommendations contained in the contractor's IV&V report and will make the appropriate revisions to its ongoing reaccreditation efforts to ensure that certification and accreditation efforts (C&A) are properly documented and cross-referenced.

Recommendation 6: Develop a Department-wide configuration management plan/security configuration policy.

Status: Corrective Action Still in Process. Configuration management has been addressed in the recently published VA Handbook 6500. Additional policy regarding this issue still needs to be developed.

To date the following actions have been completed regarding implementation of a configuration management plan for the VA enterprise: (1) current configuration management practices have been gathered (August 2007), (2) the current status of the VA configuration management program policy and handbook have been determined (July 2007), (3) a configuration management working group charter, process, and list of deliverables has been established/developed; and (4) a configuration management working group has been established and a working group lead has been identified (December 2007).

Tasks that still need to be accomplished are: (1) a review of all current configuration management practices across the VA enterprise (target completion date is late March 2008), (2) development of VA configuration management policy (target completion date is May 2008), (3) development of configuration management plans to support change control procedures (target completion date is November 2008), and (4) execution of configuration management implementation and training plans VA-wide, target completion date is September 2009.

Recommendation 7: Verify information categorization and risk assessments relating to sensitive information are in accordance with FIPS 199.

Status: Corrective Action Still in Process. VA IT Directive 06–1, *Data Security—Assessment and Strengthening of Controls,* dated May 24, 2006, established a program to remediate the IT security deficiencies. The DS–ASC plan, was developed to address deficiencies. VA has established a data control board to classify VA data which will assist in the implementation of this recommendation.

Recommendation 8: Develop and fully implement procedures for protecting sensitive information accessed remotely or removed from VA facilities in accordance with NIST SP 800–53.

Status: Corrective Action Still in Process. VA IT Directive 06–1, *Data Security—Assessment and Strengthening of Controls,* dated May 24, 2006, established a program to remediate the IT security deficiencies. This is already being partially addressed through the introduction of new software.

Recommendation 9: Complete the implementation of two-factor authentication in accordance with NIST SP 800–53.

Status: Corrective Action Still in Process. VA IT Directive 06–1, *Data Security—Assessment and Strengthening of Controls,* dated May 24, 2006, established a pro-

gram to remediate IT security deficiencies. This issue has been provided to DS–ASC personnel for incorporation into the DS–ASC program. A consolidated program for identity management has already been established to partially address this deficiency.

A target date has not been established. With the initiation of the DS–ASC contract award, milestones are being developed and target dates will be established in the next 2 or 3 months.

Recommendation 10: Identify solutions and an implementation plan for a workable time-out function for remote access through VPN in accordance with NIST SP 800–53.

Status: Corrective Action Still in Process. While this recommendation is being addressed in the DS–ASC, it cannot be currently implemented as the 30 minute timeout feature for inactivity does not always work as intended with technology currently deployed. This limitation can be attributed to the frequent system activity caused by certain software products (e.g., host based IPS) which makes the VPN connection appear to be active, therefore never reaching the 30 minutes threshold of inactivity.

While the applications in use do timeout, the VPN sometimes does not. VA feels that the timeout capability provided by the current suite of deployed software is enough to mitigate this risk. VA will search for solutions to this issue in its next generation of RESCUE software.

Recommendation 11: Complete implementation of security control measures involving access to sensitive information by non-VA employees.

Status: Corrective Action Still in Process. This recommendation is being added as a task to the DS–ASC and will address the five areas of improvement identified in the OI&T August 25, 2006 briefing to the former Secretary.

Recommendation 12: Implement a standardized security program for use by all of VA's national and regional data centers to facilitate more consistent security program assessment and monitoring.

Status: Corrective Action Still in Process. A standardized security program for the data centers will be developed and implemented.

Recommendation 13: Institute mechanisms to notify all VA facilities of the specific security issues identified in this report and from future testing so that appropriate corrective actions can be taken on these issues if they exist at other facilities.

Status: Corrective Action Still in Process. The OIG FY 2006 FISMA audit report has been distributed to personnel who have overall responsibility for implementation of corrective action (champions and project managers) shown in the data security-assessment and strengthening of controls (DS–ASC) program. This report, and all subsequent similar reports, will be posted to the VA Intranet by the end of March 2008 so that deficiencies identified in these reports can be made available to OI&T personnel located at other VA facilities. An e-mail will be sent notifying OI&T personnel of each report's availability and VA Intranet location.

Question 3: What has been accomplished since June 2007 in fully implementing the IT Governance plan? Are all governance boards in place and operating?

Response: Implementation of the IT governance plan is the responsibility of the VA Executive Board, the Strategic Management Council (SMC) and VA senior leadership; not just OI&T. IT governance is an integral part of VA-wide governance and aligns to VA's business strategies and objectives. Trust must be built among the stakeholders in the management of IT in VA. Implementing VA IT governance involves shared decisionmaking through the IT governance boards, based on the guiding principle of aligning IT strategy and goals to business strategy and goals.

Since June 2007, each of the IT governance boards played an integral part in identifying and prioritizing the myriad requirements that the business units have to contend with. The Planning, Technology and Services (PATS) Board developed the FY 2009 program with input from the business units and stakeholders. The Business Needs and Investment Board (BNIB) developed FY 2008 execution strategy and FY 2009 funding recommendations. The Information Technology Leadership Board (ITLB) carried the message of the PATS and BNIB to the highest levels of VA's leadership and recommended that the Deputy Secretary approve the IT budg-

ets. The FY 2009 budget submission was unanimously approved by the SMC/VA Enterprise Board (VAEB).

Question 4: With respect to the VistA outage on August 31, 2007, described in the testimony of Dr. Volpp, please state what actions are being taken to ensure that such an outage does not occur in the future. In addition, state whether the "failover" function between the two western data centers is sufficient to ensure uptime of VistA sufficient to meet the healthcare needs of VHA, the reason(s) the "failover" function is or is not able to meet those needs, and, if the "failover" is not sufficient to meet those needs, what remediation will be undertaken.

Response: The root-cause of the outage on August 31, 2007 was lack of adherence to change management procedures by VA staff. Staff has been retrained in change management procedures and compliance is being closely monitored. Senior management have communicated to staff that any future outage with similar cause may result in disciplinary actions against those individuals not adhering to the procedures.

The "failover" function is in place and able to meet the healthcare needs of VHA in this region. Failover capability has been successfully tested as recently as September 16, 2007.

Failover capability is a core system design requirement of the regional data processing program and as such is available if an event occurs that warrants that action. The design is intended for disaster situations. Although it takes up to 4 hours to failover once the decision is made to do so, sites do have "read only" capability available. During the August 2007 outage, "read only" capability was available to all affected sites.

The outage that took place on August 31, 2007 at the west coast Regional Processing Center (RPC) in Sacramento was precipitated by a change that was made to the running environment without formal approval. Additionally, this unapproved change was made incorrectly—resulting in a number of systems being taken offline, rendering the entire system unavailable. Based on detailed analysis, the Department is instituting a number of improvements and architectural changes to the RPC on the west coast in order to ensure efficient day to day processing, increased availability and enhancement of failover of resources in the event of a disaster. The RPC was originally architected to ensure continuity of operations during a Katrina like episode or other regional disaster. The Department has also engaged a contractor for an independent analysis of the RPC. The results of that engagement have not been delivered as of yet. This information will also be used to validate or enhance the department's architectural decisions.

These changes in the RPC environment will ensure that VA moves closer to a more highly available environment for the VistA systems that serve the Department's medical centers and clinics. Already, the RPC on the east coast is providing very high availability. The scheduled and unscheduled downtime metrics for VistA in those data centers fall into the "Best In Class" category as defined by Gartner—their most stringent category. While hardware augmentation and realignment of systems will improve availability in the west coast data centers and with the VistA platform design in general—it should be noted that the Department's aging VistA application must also be examined.

The Department has launched an assessment team to review "Class 3" applications. It is believed that certain class 3 code can negatively affect the health and performance of a running VistA system. The team embarked upon its analysis at a VA facility—the San Francisco VAMC—where the presence of Class 3 code is significant. We are examining efficiency of Class 3 code, adherence to standards, and scalability qualities—in order to ensure efficient use ability at a RPC.

In closing, we believe the availability needs of the organization will be met by the continued application of engineering enhancements to the RPC infrastructure as well as the analysis and renovation of Class 3 code. Disaster recovery failover capabilities have been in place since the launch of the RPCs and will also continue to be enhanced by the engineering changes being implemented already, with others on the immediate horizon. In the end, however, the application is what dictates, in great part, limitations on performance and availability. The current VistA application has roots and elements that are more than 20 years old. Until the advent and full deployment of HealtheVet—which brings significant renovation of the aging VistA code by rearchitecting using industry best practices including Service Oriented Architecture (SOA)—overall availability for VistA can be optimized only to a point but will still fall in Gartners's "Outstanding" or "Best in Class" categories.

Question 5: GAO identified "dedicating an implementation team to manage change" as a critical success factor to the department's implementation of a central-

ized structure. The department is currently managing the realignment through two organizations: the Process Improvement Office under the Quality and Performance Office and the Organizational Management Office. The Executive Director of the Organizational Management Office has recently resigned his position, leaving one of the two offices without leadership. Please explain the following:

Question 5(a): Why did VA decide to manage the realignment through two organizations rather than dedicating a single implementation team to manage change? What is the benefit to having two organizations over one?

Response: Since the executive director of the Organization Management Office resigned, the deputy director of the Office of Quality and Performance has been assigned the responsibility to advise the principal deputy assistant secretary (PDAS) and Assistant Secretary for OI&T on realignment issues in addition to continuing the process improvement effort.

Overall, IT executive leadership team is responsible for meeting established performance goals related to the implementation of the IT realignment. For example, the Information Protection and Risk Management (IP&RM) organization is responsible for ensuring proper policies and procedures are in place to protect personally identifiable information of both veterans and employees, as is ITOC. The Resource Management (RM) organization is responsible for career management, funds execution and asset management. Similarly, the Office of Enterprise Development (OED) ensures appropriate processes are implemented as IT products are developed, Enterprise Operations and Infrastructure (EO&I) is measured on their compliance to service level agreements and the Office of Enterprise Strategy, Policy, Plans and Programs (OESPP&P) ensures multi-year programming and project management activities are implemented as well as developing and describing IT strategic plan goals. Each component of OI&T has developed performance metrics, which will be tracked and managed to ensure goals are met and performance shortfalls identified. Additionally, processes for the 36 major IT business areas have been defined and are in the initial implementation stages. Recently, OI&T has streamlined the organizational management of the realignment to one office, the Office of Quality and Performance. This organization will be responsible for ensuring IT process implementation, performance management, as well as program evaluation and analysis and will advise the PDAS and Assistant Secretary for OI&T on realignment performance goals and areas for improvement.

Question 5(b): Who will be held responsible in tracking implementation goals and identifying performance shortfalls? Who will be held accountable if the implementation goals are not met and performance shortfalls are realized?

Response: Overall, the IT executive leadership team is responsible for meeting established performance goals related to the implementation of the IT realignment. For example, IP&RM organization is responsible for ensuring proper policies and procedures are in place to protect personally identifiable information of both veterans and employees, as is ITOC. The RM organization is responsible for career management, funds execution and asset management. Similarly, OED ensures appropriate processes are implemented as IT products are developed, EO&I is measured on their compliance to service level agreements and OESPP&P ensures multi-year programming and project management activities are implemented as well as developing and describing IT strategic plan goals. Each component of OI&T has developed performance metrics, which will be tracked and managed to ensure goals are met and performance shortfalls identified. Additionally, processes for the 36 major IT business areas have been defined and are in the initial implementation stages. Recently, OI&T has streamlined the organizational management of the realignment to one office, the Office of Quality and Performance. This organization will be responsible for ensuring IT process implementation, performance management, as well as program evaluation and analysis and will advise the PDAS and Assistant Secretary for IT on realignment performance goals and areas for improvement.

Question 5(c): Who is currently advising and assisting the CIO since the Executive Director of the Organizational Management Office resigned?

Response: The Deputy Director of the Office of Quality and Performance is assigned the responsibility to advise and assist the Principal Deputy Assistant Secretary and Assistant Secretary for IT on realignment issues.

○