ASSESSING INFORMATION SECURITY AT THE U.S. DEPARTMENT OF VETERANS AFFAIRS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

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

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MAY 19, 2010

Serial No. 111–78

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE
57–022 WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

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

CONTENTS

May 19, 2010

ASSESSING INFORMATION SECURITY AT THE U.S. DEPARTMENT OF VETERANS AFFAIRS

WEDNESDAY, MAY 19, 2010

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

The Subcommittee met, pursuant to notice, at 10:06 a.m., in Room 334, Cannon House Office Building, Hon. Harry E. Mitchell [Chairman of the Subcommittee] presiding.

Present: Representatives Mitchell, Space, Walz, Alder, and Roe.

Also Present: Representative Buyer.

OPENING STATEMENT OF CHAIRMAN MITCHELL

Mr. MITCHELL. Good morning and welcome to the Committee of Veterans' Affairs Subcommittee on Oversight and Investigation hearing on Assessing Information Security at the U.S. Department of Veterans Affairs (VA). This hearing will come to order.

I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and that statements may be entered into the record. Hearing no objection, so ordered.

Today we will examine the current status of information security at the VA and its ability to protect itself against both malicious and accidental sensitive information breaches.

The Department of Veterans Affairs employs a sophisticated computing infrastructure to store the health and financial records of millions of American veterans and their families. Each day, there is the potential for millions of attempts to gain unauthorized access to government computers that hold this information through unsecured ports and other means.

The risks to the VA of not implementing a sound information security program are considerable and, unfortunately, have already been seen through several situations in the past.

Just recently we have learned of two data breaches. In Texas, 3,265 veterans' records were compromised when information went missing from a facility conducting lab tests. In a second instance in Texas, a VA contracted company had a laptop stolen, comprising the records of 644 veterans.

These recent data breaches are proof that VA still has a long way to go in ensuring our Nation's veterans that their most sensitive information is being safely stored and handled.

The Federal Information Security Management Act of 2002, or FISMA, is a critical and evolving mandate designed to help Federal

Government entities, including the VA, protect personally identifiable and otherwise sensitive information.

In March of this year, the Office of Management and Budget (OMB), released its fiscal year 2009 report on FISMA. Unfortunately, the VA ranked dead last among other FISMA monitored agencies in areas such as the percentage of log-in users trained on information security awareness and also in the issuance of personal identity verification.

Additionally, the OMB report also lists that VA is one of six Federal agencies identified as having a material weakness.

It is clear that the VA has a wide range of areas in which it must improve its information security infrastructure. Strengthening interagency network connections, access to controls, and improving configuration management are some of the things that will yield positive results in securing VA's computing network.

In light of the recent data breaches in Texas and OMB's recent release of its fiscal year 2009 FISMA report, there is no better time to review VA's information security posture and hear from the Department on how they plan to address the challenges they face securing the personal information of our Nation's veterans.

I am pleased that both the VA Office of Inspector General (OIG) and the U.S. Government Accountability Office (GAO) are here to shed light on additional improvements that the VA can make. I look forward to their testimony.

[The prepared statement of Chairman Mitchell appears on p. 32.]

Mr. MITCHELL. Before I recognize the Ranking Republican Member for his remarks, I would like to swear in our witnesses. And I ask all witnesses from both panels to please stand and raise their right hand.

[Witnesses sworn.]

Mr. MITCHELL. Thank you.

I would now like to recognize Dr. Roe for opening remarks.

OPENING STATEMENT OF HON. DAVID P. ROE

Mr. ROE. Thank you, Mr. Chairman, and I appreciate you having this very important hearing.

And before we start, I would like to introduce a very close friend of mine, a highly decorated Vietnam veteran who is visiting in Washington, Mack McKinney.

Mack, if you would stand. I certainly appreciate your service.

[Applause.]

Mr. ROE. Mack is a Sergeant Major. And, Ranking Member Buyer and Mr. Chairman, Mack did it on the ground in Vietnam. And thank you for your friendship.

The security of the information the Federal Government has under its purview is of high importance. Recognizing that importance, Congress passed several Acts to increase security awareness throughout Federal agencies including the Department of Veterans Affairs.

In 2002, Congress passed the Federal Information Security Management Act, which permanently reauthorized the framework laid out by previous legislative initiatives such as the Computer Security Act of 1987, the Paperwork Reduction Act, that must be the oxymoron of all oxymorons right there, the Information Technology

Reform Act of 1996, and the Government Information Security Reform Act of 2000.

The enactment of FISMA was a critical step to ensure the continuation of requirements and, therefore, the ability to effectively identify and track the Federal Government's information and security system status.

Prior to 2001, the VA Office of Inspector General and other outside agencies had expressed concern and identified material weaknesses regarding information security management at VA.

Since 2001, OIG reviews of VA FISMA compliance continued to identify significant information security vulnerabilities that placed VA at risk of denial of service attacks and disruption of mission critical systems and unauthorized access to sensitive data.

Numerous security weaknesses were identified, but generally not corrected by VA even after the OIG identified repeated weaknesses over several years.

One glaring example of this state of affairs was demonstrated by a fiscal year 2004 report where the OIG made 16 recommendations to VA to strengthen information security management, which remained opened at least up until May 23rd, 2006.

Since the data breach of May 2006, the second largest in the Nation and the largest in the Federal Government, we have seen the centralization of VA's information management including information security.

These efforts have continued through the current Administration under Assistant Secretary Baker's lead. I appreciate the massive undertaking by both the previous Administration and the current Administration to tighten the controls on protecting the data of our Nation's veterans.

However, while progress has been made in centralizing the information technology (IT) Department at the VA, I am uncertain how much progress has been made in protecting information managed by the Department.

In reviewing the FISMA reports issued by OMB over the past 7 years, I am concerned about the VA's status with respect to information security.

In May of 2006, the VA did not even file a report on its FISMA compliance.

In 2007, the VA received an F on its FISMA compliance.

Most glaring is the recent 2009 FISMA report which shows that even though VA has over 500 FTEs assigned to security related duties, it had the lowest percentage of log-in users trained in information security, 65 percent, and the lowest percentage of personal identifying verification credentials issued by the Agency, less than 5 percent to employees and contractors.

I am highly concerned that VA is just not taking information security seriously enough. The protection of the personal information of our Nation's veterans should be a high priority at the Department. We do not want another security breach at the Department and we certainly do not want another one that would reach the level of the May 2006 breach. But if VA continues on its current path, we may just have that.

On April 28th, 2010, my staff was alerted to a stolen laptop which had access to VA medical center data. This contractor owned

the laptop, which was unencrypted and possibly contained the personal identification information of approximately 644 veterans.

Upon further investigation, we learned that in November 2009, the Department issued a directive for VA to incorporate VA Acquisition Regulations (VAAR) Clause 852.273–75, which provides security requirements for unclassified information technology resources.

The VA reviewed 22,729 contracts to determine whether the contracts required the inclusion of this clause. Sixty-four hundred required the inclusion of VAAR contracts that has the clause inserted. That is 88 percent. Five hundred and seventy-eight contractors refused to sign the clause, 9 percent, and an additional 197 still require the clause.

I have many questions over this issue, some of which I hope we can answer in today's hearing.

Why was the clause not enforced prior to 2009?

Did Heritage Health Solutions have the clause included in their contract?

What are VA's plans as far as the 578 contractors who refuse to sign the clause when added to their contract? Number four, what was the primary reason that most of the contractors refused to sign on to the additional clause? And, finally, what is VA going to do to tighten the controls on contractor-owned equipment that is regularly accessing the VA networks and storing data related to our Nation's veterans?

To place our veteran information at risk is irresponsible. These men and women have fought for our Nation, have placed their own lives in jeopardy to secure our freedom, and we repay them by tossing caution to the wind with respect to their personal information. This is totally unacceptable.

VA must take immediate action to secure our veterans' information and to ensure that all contracts requiring access to any data at the VA include the protections our veterans need and require.

Thank you again, Mr. Chairman, and I yield back.

[The prepared statement of Congressman Roe appears on p. 32.]

Mr. MITCHELL. Thank you.

Mr. Walz.

Mr. WALZ. I will yield.

Mr. MITCHELL. Okay. Mr. Buyer.

OPENING STATEMENT OF HON. STEVE BUYER

Mr. BUYER. Mr. Chairman, I would ask unanimous consent that I may participate in today's hearing and I will ask questions at the end of all Members of the Committee.

Mr. MITCHELL. Without objection.

Mr. BUYER. I would also ask unanimous consent to give an opening statement.

Mr. MITCHELL. Without objection.

Mr. BUYER. All right. Thank you very much.

I appreciate you allowing me to join in the O&I Subcommittee hearing. As you know, the protection of personal information of the Nation's veterans has been a high priority of mine actually for the last decade.

During the 109th Congress, in order to address the serious deficiencies in data protection for personally identifying information

maintained by the VA, I introduced legislation entitled the "Veterans Identity and Credit Security Act of 2006", H.R. 5835, which passed the House by a vote 408 to zero.

This legislation was later incorporated into legislation that became Public Law 109–461. It is my hope that this Public Law would provide the VA with the necessary tools with which to combat information security flaws at the VA.

In August of 2006, the VA issued VA Directive 6500, which detailed the steps by which the Department would provide compliance with system security measures.

And on September 18th of 2007, the Department issued national rules of behavior for employees and contractors to use as a means to secure the data contained in VA's information systems.

Upon further investigation, we learned that in November of 2009, the Department issued an additional directive for VA to incorporate VA Acquisition Regulation 852–273.75 into all contracts where this type of information might be accessed.

I applaud Secretary Shinseki and Assistant Secretary Baker for taking these measures to protect our Nation's veterans and their personal information. Unfortunately, the recent data breaches in April are a stark reminder that the VA and Congress must always be vigilant in protecting this information wherever it may exist.

The details of these breaches clearly indicate that the VA is still unable to adequately protect veterans' personal information. It also shows that senior managers do not know what their responsibilities are and that responsibilities are not clearly defined especially between the contracting process and the information security management process.

So that is why, Mr. Chairman, I am really pleased that you have not only our Chief Procurement Officer here but also our Chief Information Officer (CIO) so we can understand the delineations of their responsibilities.

Mr. Chairman, I am here to determine if there was something we missed in the legislation that we passed 4 years ago. So I am hopeful that the Administration can advise us if there are any particular needs or if, in fact, there are problems with the legislation or where did we go wrong. How do we improve this situation? And I also want to hear about where we go about fixing the current situation with regard to the contracts.

This most current breach involves a contractor that had 69 contracts in 13 Veterans Integrated Service Networks (VISNs) involving over 30 VA medical centers. Twenty-five of these contracts were missing security clauses. The contractor signed all certificates of compliance. Nobody at the VA checked and verified to my knowledge. I want to know who at the Veterans Health Administration (VHA) was asleep at the wheel. Where is the accountability and, in fact, who is accountable, who is responsible?

When Secretary Shinseki ordered a review of 22,729 VHA contracts last February, over 6,000 were missing the basic IT security clause. These contracts were modified over a period of 7 months to include the security clauses. It appears to me that no one at VHA contracting verified any compliance in spite of certificates of compliance by contractors. Disciplined contracting in the VA is dysfunctional and clearly broken. It is highly decentralized and with

almost total absence of contract review or oversight. What is going to happen to the 578 contractors who refused to sign the modification to their contracts to put the information security clause in place?

And who is going to step forward and pay for such compliance if, in fact, they do not want to or if we have got ourselves in a position whereby maybe they are providing a particular medical service, and I am leaning over to the VHA, to say that the service that they provide is so important, yet they refuse to sign the clause, what are you going to do and who is going to pay for what or do they feel that they have leverage over us that we are going to pay for the IT?

I do not know. I am interested to see how you are going to be able to work that out or if you are going to have to reprogram monies or you have got monies to be able to do this type of thing.

I want to thank you, Mr. Chairman, for holding this hearing and to the Ranking Member.

The record clearly shows that on May 6th, 2006, the data breach occurred. This was the largest in the Federal Government and the second largest in American history. This Committee worked side by side in a bipartisan manner to strengthen the IT security at VA. And I look forward to working with you to resolve this matter.

I also want to thank Roger Baker. You stepped forward into the breach. I am not here to beat you up at all. I recognize that this is work in progress. This is maintenance. And I am not downplaying this. I know this is a very large system. We worked very hard to centralize this IT.

I also recognize that you have not had the most cooperation or the best effort of cooperation from VHA over the years. You know, they have done everything imaginable in my personal opinion to derail the centralized effort. And they also have not been as forthcoming with regard to security compliance and assurances that I think they should.

So you stepping into this breach, accepting responsibilities, and then you ensuring that not only your eyes but the eyes of the men and women who then serve directly under you in your lines of authority put their eyes at the VISN and the medical centers into that process extremely important.

And you recognize that. And I want to applaud you for doing that. So when your CIO at the medical center wants to put their eyes into that medical contract and the Chief Medical Officer then sitting at that board table said get your nose out of my business, no, no, no, no, no, no. It is your business.

And you were in the room when we designed this. And that is why I am glad that you are in charge when problems arise too. So you and I and this Committee are on the same page. And I applaud you for that.

I also want to thank the GAO and the OIG for your work. I read your reports last night.

Thank you, Mr. Chairman. I yield back.

Mr. MITCHELL. Thank you.

At this time, I would like to welcome panel one to the witness table. And joining us on the first panel is Greg Wilshusen, Director of Information Security Issues at the U.S. Government Account-

ability Office, accompanied by Valerie Melvin, Director of Information Management and Human Capital Issues.

I would also like to welcome Belinda Finn, Assistant Inspector General for Audits and Evaluations, Office of Inspector General, U.S. Department of Veterans Affairs. Ms. Finn is accompanied by Michael Bowman, Director of Information Technology and Security Audits in the Office of Inspector General.

I ask that all witnesses stay within 5 minutes for their opening remarks. Your complete statements will be made part of the hearing record.

At this time, I would like to welcome and recognize Mr. Wilshusen.

STATEMENTS OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY VALERIE C. MELVIN, DIRECTOR, INFORMATION MANAGEMENT AND HUMAN CAPITAL ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; AND BELINDA J. FINN, ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY MICHAEL BOWMAN, DIRECTOR, INFORMATION TECHNOLOGY AND SECURITY AUDITS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Chairman Mitchell, Members of the Subcommittee, thank you for the opportunity to participate at today's hearing on VA's information security program.

Since 1997, GAO has identified information security as a governmentwide high risk issue. This has been particularly true at VA where the Department has been challenged in protecting the confidentiality, integrity, and availability of its computer systems and information.

At previous hearings before this Subcommittee, we have testified on some of these challenges. Today we will discuss VA's progress in implementing information security and complying with FISMA.

Mr. Chairman, for over a decade, VA has faced long-standing information security weaknesses that have left it vulnerable to disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Nevertheless, the Department has made limited progress in resolving these weaknesses.

In September 2007, GAO reported that shortcomings in the implementation of several departmental initiatives to strengthen security could limit their effectiveness. At that time, we made 17 recommendations for improving the Department's security practices including, for example, developing guidance for its information security program and documenting related responsibilities.

VA has implemented five of those recommendations and has efforts underway to address 11 of the remaining 12. We plan to follow-up this year with the Department to determine whether it has fully implemented our recommendations.

For the 13th year in a row, VA's independent auditor reported that inadequate system controls over financial systems constituted a material weakness in fiscal year 2009. Among 24 major Federal agencies, VA was one of six to report such a material weakness.

Deficiencies were reported in each of the five major categories of information security controls including, for example, access controls, which are intended to ensure that only authorized individuals can read, alter, or delete data, configuration management controls which provide assurance that only authorized programs are implemented, and segregation of duties which reduce the risk that one individual can independently perform inappropriate activities without detection.

Also for fiscal year 2009, the VA Office of Inspector General designated the Department's information security program as a major management challenge. Of 24 major agencies, VA was 1 of 20 to have information security so designated.

In March 2010, we reported that Federal agencies including VA had made limited progress in implementing the governmentwide initiative to deploy a standardized set of configuration settings on Windows workstations. We determined that VA had satisfied certain requirements of the initiative but had not fully implemented other key requirements.

Accordingly, we recommended that VA, among other things, complete implementation of its approved set of configuration settings and acquire and deploy a tool to monitor compliance with those settings. VA concurred with our recommendations and indicated that it plans to implement them by September 2010.

VA's progress in implementing FISMA-related control activities has also been mixed. For example, from fiscal year 2006 through 2009, the Department reported a dramatic increase in the percentage of systems for which a contingency plan was tested. However, during the same period, the Department reported decreases in the percentage of employees who had received information security training.

Compared to 23 other major agencies, VA's performance in implementing these control activities was equal to or higher in some areas and lower in others.

In summary, Mr. Chairman, effective security controls are essential to securing the systems and information on which VA depends to carry out its mission. The Department continues to face challenges in resolving long-standing weaknesses. Overcoming these challenges will require sustained leadership, management commitment, and effective oversight.

Until VA fully and effectively implements a comprehensive security program and mitigates known vulnerabilities, its computer systems and sensitive information will remain exposed to an unnecessary and increased risk of unauthorized use, disclosure, tampering, and theft.

This concludes our opening statement. And Ms. Melvin and I would be happy to answer your questions.

[The prepared statement of Mr. Wilshusen and Ms. Melvin appears on p. 34.]

Mr. MITCHELL. Thank you very much.

Ms. Finn.

STATEMENT OF BELINDA J. FINN

Ms. FINN. Thank you, Chairman Mitchell.

Chairman Mitchell and Members of the Subcommittee, thank you again for the opportunity to discuss our work on VA's implementation of an agency-wide information security program.

With me today is Mr. Michael Bowman, Director of Information Technology and Security Audits for the OIG.

In March 2010, we issued our report on the fiscal year 2009 assessment of FISMA implementation. That report included 40 recommendations for improving VA's information security program.

Seven years after FISMA's enactment, we continue to find significant deficiencies with information system security controls that could have potentially alarming consequences.

While VA has made progress defining policies and procedures, it faces significant challenges implementing effective controls over system and network access, system interconnections, configuration management, and contingency planning practices.

For example, during our testing of access controls, we identified significant weaknesses that expose VA mission critical systems to unauthorized access. We found numerous weak or default passwords on application servers, databases, and networking devices at most VA facilities. These weak or default passwords can allow malicious users to easily gain unauthorized access to mission critical systems.

For example, using a default password, a hacker could easily access a Microsoft database with administrative rights and change data or establish a back door to allow future entry into the database.

Second, our testing of system interconnections revealed a significant number of external connections that VA had not identified and were not actively monitoring. This lack of comprehensive monitoring of these connections represents a significant risk that a hacker could penetrate the network and systems over an extended period of time without being detected.

Configuration management controls ensure that only authorized, tested, and adequately protected systems operate on our protected networks.

We identified significant problems with software updates, virus protection, and other controls that resulted in unsecure web application servers, servers hosting vulnerable third-party applications, and excessive user access on critical database platforms.

These weaknesses could again allow malicious users to exploit the vulnerabilities and gain unauthorized access to VA systems.

Finally, our review of the contingency planning processes revealed many instances where VA facilities did not validate that personnel could restore mission critical systems at a remote processing site as planned. Without in-depth and realistic contingency plan testing, VA cannot be certain that it can readily restore systems in the event of a disaster or service disruption.

Weaknesses in information security, policies, and practices can expose critical systems and data to unauthorized access and disclosure.

While VA has made progress defining policies and procedures, implementing effective controls to protect systems and data from

unauthorized access, alteration, or destruction represents a significant challenge in VA's highly decentralized and complex infrastructure.

We believe that the VA systems will remain at increased risk until VA fully addresses our recommendations and implements an effective information security program.

Mr. Chairman, that would conclude my oral statement. Mr. Bowman and I will be happy to answer any questions that you or other Members of the Subcommittee may have.

[The prepared statement of Ms. Finn appears on p. 40.]

Mr. MITCHELL. Thank you.

Mr. Wilshusen, we learned recently of an incident in which the VA contractor's laptop, their computer that was unencrypted with veterans' information was lost or stolen.

What can the VA do to ensure that its contractors effectively secure the system and information that they operate or process on the VA's behalf? And is the VA doing anything about this?

Mr. WILSHUSEN. Well, as you know, under FISMA, agencies are responsible for assuring the security over their systems and information including those that are operated by contractors and other third parties or information that those contractors and third parties possess on behalf of the Agency. VA can do a number of things and should be doing a number of things to protect that information.

First of all, it should be including and incorporating security requirements into its contracts with its contractors. It should also assure and require that contractors certify that they are meeting the requirements of the contract.

But, importantly, it should also establish mechanisms for an independent confirmation that contractors are actually performing as they should be and as they are required to do under the contract.

Clearly establishing and implementing a mechanism for monitoring contract performance and compliance will be critical to assure that agencies, I am sorry, that contractors are implementing those controls.

And then if there are instances where contractors are not complying with the required security measures, then they should be held accountable.

And that is one of the areas, as I understand it, even though we have not yet looked at VA's actions in this area at present, the last we looked at VA was back in September 2007 where we identified a number of vulnerabilities with its information security program, but that is one area certainly that is important for VA to assure that contractors are implementing the appropriate security requirements over its information systems.

Mr. MITCHELL. It seems like several of the high-profile data breaches affecting veterans' information occurred as a result of physical theft of IT resources such as a laptop computer or thumb drive.

What can the VA do to protect veterans and itself from these types of security incidents?

Mr. WILSHUSEN. Well, you are absolutely correct. For example, the May 2006 data theft involved the physical theft of an external hard drive and laptop as well as the more recent one from the con-

tractor. And, indeed, that across government is one of the types of incidents that results in significant data loss.

And what VA can do is a number of things. One is ensuring that those laptops have strong authentication on them that require, for example, two factor authentication. So someone who steals a laptop would need to not only know a particular piece of information such as a password or a PIN number but also possess either a token or some sort of biometric that would allow only one user then to access and authenticate to that system.

Certainly another key point is encrypting the data on the laptop. That is essential. VA has made progress with that on the Agency's laptops.

In 2007, we did a test where we tested 248 laptops at eight locations and found that they had encrypted the laptops for 244, about 98 percent of the laptops. But those were Agency laptops. Where they often have had issues is when the contractors have not encrypted data on the laptops.

Another key thing is just to limit and restrict the amount of sensitive information that is contained or stored on these laptops. They should only—the information should only be on the laptop for the limited period of time that is required and the amount of sensitive information should only be stored on the laptop to the extent that it is for authorized, legitimate business purposes.

Other types of controls that should be in place on laptops include just general maintenance including that they have intrusion prevention systems or personal firewalls on the laptops, that the laptops are protected with current antivirus software, and all security patches have been installed on those systems.

Mr. MITCHELL. Thank you.

Dr. Roe.

Mr. ROE. Thank you. Thank you, Mr. Chairman.

Obviously the VA has an enormous job in managing hundreds of millions, if not billions of bits of information. And let me suggest to you that that is a good thing because one of the problems we have had is being able to quickly get claims done and this is important.

The advantage of paper is you cannot haul out 26 million of them under your arms and carry them out. You just physically cannot do it. So before the VA was slow, but it was very difficult to lose much information. Someone might take a chart or two home, but they are not going to take 26 million of them home like a guy did on his laptop.

And it appears to me that the problem is that we do not or have not had adequate encryption and so forth on all the pieces of information. And it is important sometimes for these folks to take the work home.

Let me give you an example. A physician friend of mine at the VA, he is not allowed to take his laptop away with him, which he would go away for, let us say, a week or two vacation. He would work at that time and expedite things. He is a gastroenterologist. He is a consultant. They are way behind on those consults. He could do a lot of work. But he cannot take it with him because of this issue that occurred with the 26 million people.

And it is also incredibly expensive when that happened. I know I was one of the veterans who got the letter. And I think one mail-out was $14 million. Two mail-outs went out. That was $28 million to let veterans know that, hey, guess what, we goofed, we let your information with your Social Security number and so forth get out there on the World Wide Web. Not a real good feeling. And I think we have to do better.

I guess one of the questions I have, and you made some great points in here and in your testimony, your written testimony, the VA continues to report significant information security shortcomings and you go through these, and my question is, why have they not been corrected? I mean, it has clearly been pointed out, so why has it not been done?

Mr. WILSHUSEN. I think there is probably a number of different reasons why they have not. One of the issues is in years past, VA has been decentralized, particularly with the organization of responsibilities for information security. With the 2006 legislation and bill, I am sorry, Act that was passed, that helped to centralize some of that responsibility within the CIO's and Chief Information Security Officer's (CISO's) offices. And that was a key moment, I think.

Certainly another key area is prior to May 2006 when that incident occurred, the emphasis on information security may not have been as great as subsequent to that. So since 2006, there has been some progress. Certainly they now have very capable individuals in place as Congressman Buyer has pointed out with the new CIO.

Mr. ROE. I guess the question I have with that is this, is that the FISMA Act had been passed along with——

Mr. WILSHUSEN. Oh, yes.

Mr. ROE [continuing]. Four or five things I mentioned ahead of that time, it appears that nobody was paying any attention to the problem and did not take it seriously and still, even after a huge breach like that, apparently not serious enough that it is still not going on.

And, Ms. Finn, just a thought occurred to me when you were speaking. You raised a tremendous point. If a hacker, because our Web site was hacked in my office here in DC, if you could hack into a VA data system and you said, I think, in your testimony that you could change information, could you change information about me as a veteran if I am in that system and then file a false claim? It looks to me like that would be easy to do if the data were changed.

Ms. FINN. I would say if a hacker got into that particular database, that quite likely they could do that.

Mr. ROE. So you could go in there and change your information about where you served or what disability you might have? I mean, that is a tremendous opportunity for fraud.

Ms. FINN. Yes. I will say that I do not know that we saw specific vulnerabilities in those large databases.

Mr. ROE. I guess my question was, if you do not have the security system, because, I mean, everybody's e-mail has a password and a user name, and is there any way to know that that has happened? I mean, could it have been breached and anybody not even know?

Ms. FINN. Yes, it could have.

Mr. BOWMAN. We did work on some of those mission critical systems and we found instances where audit logs were not being maintained. So if systems were actually infiltrated, there were not records identifying that and responding to it.

We also identified instances where the databases on some of these larger systems did have default credentials. So probably the risk is more from the internal threat than it is from the internet, but the threat does exist.

Mr. ROE. I think the reason, before I yield back, Mr. Chairman, I think this is important because as a physician, we make decisions based on what is in those records. And if those records are manipulated in a negative way, you will end up making very bad decisions. The more I listen to this and read the testimony last night, the more critical I realized this was to get this right.

So I yield back.

Mr. MITCHELL. Thank you.

Mr. Walz.

Mr. WALZ. Thank you, Mr. Chairman and Ranking Member Roe, and the Ranking Member of the full Committee, for your attention to this and your work on it.

I, like Dr. Roe, was one of those veterans that received the letters and I hear much about this.

I want to thank all of you for your commitment and public service and also your commitment to good governance and oversight and to all of our folks here from the VA. This room is absolutely committed to the best care of our veterans. That goes without question. We are here to figure out how to do that.

So, Assistant Secretary Baker, I share the Ranking Member's admiration for you. And I guess he used the right term in this regard, stepping into the breach. And I do appreciate that.

A couple questions I have. And in recognizing that we are making progress and where there is other things, my concern and where I am coming from, the broken record in me, as we move forward to the smart policy of seamless transition, this issue is going to become even more important, the idea of the virtual lifetime record, the electronic record, the idea of sharing between U.S. Department of Defense (DoD) and VA have become even more important.

And I am trying to find out here that balancing absolute security and access because one of the problems I find in rural areas is the access issue for our county veteran service officers and things like this.

I just came from a meeting where I sat down purposely to talk of this information security side from the private sectors with Thomson Reuters folks. And they were talking about, yes, the encryption, yes, all those things, but also the credentialing side of things, that there is that other level of safeguard of who has got access to this and why.

I guess my question is, and this might be to Ms. Finn, have any of these breaches occurred with people like in my State, one of the 26 States that has county veteran service officers, are co-located veterans service organization (VSO) representatives at the VA, have any of the breaches of data come out of those folks? Can you speak to that with any authority?

Ms. FINN. No, sir. I am afraid I cannot. I would have to do some research in order to answer your question.

[The VA OIG subsequently submitted the following information:]

In response to your question, we contacted VA for information related to security incidents. VA provided the OIG with information on security incidents for the period of February 2010 through May 2010. During this limited period, no cases of VSOs gaining unauthorized electronic access to VA's internal systems and networks were reported. However, in one instance, an individual misused authorized access to the Patient Inquiry Database. We understand that the Office of Information and Technology is working to limit access to the database so that a similar incident does not occur again. To answer the question for a broader time period, we would have to defer to VA to provide any additional information.

Mr. WALZ. Well, if we could get that because I think we are seeing the answer is, is there have not been any.

And my question is, I have limited access for these folks even something as simple as a DD–214 and then you get into the compensation and pension side of things that we need to speed the transition for benefits. My experts, my veterans, my folks that are county veteran service officers are being denied access on the basis of it could be a security breach.

As we move forward on this and as you hear details and as we find wherever our Achilles heel is in strengthening this, we have to be very cognizant of we can lock this stuff away in a vault, but if the right people do not have access to see it, we still cause damage to our veterans. And I want to know how we get that. And I do not know if anyone has any comments.

The Ranking Member brought up a great point in seeing that this might be an opportunity with the DoD folks or whatever to strengthen that. I guess maybe I was being a little more pessimistic and seeing that this is going to compound the problem and make it more difficult.

Do you see this as a challenge or an opportunity? And maybe when Assistant Secretary Baker and his folks come up, they may comment too.

Mr. WILSHUSEN. I would say it is both an opportunity and a challenge. Certainly the sharing of information will help get information to the people who need it when they need it and making sure that the information is accurate at that time.

It is also a challenge, though, to assure that those individuals only receive the information that they need and to assure that they are the correct people in receiving that information. And that is where with information sharing and providing appropriate security, there is always that balance.

Mr. WALZ. Do we do a good job on this credentialing or who has this? I keep hearing of these contractors and stuff. I am wondering, do these people need to—there are cases where they need to take it home. I think Dr. Roe is right.

But are we credentialing the right people? Is there that side of the security or is this all a software physical infrastructure side of things issue or is it more of a cultural attitude on protection of data?

Could anyone speak to that as you see it?

Ms. FINN. I think it is definitely a cultural issue and that has been the biggest change that I have seen in VA over the last 3½ years in information security. The struggle to establish the policies

and procedures that addressed, the need for encryption on devices was huge. And it was a big culture shift.

Mr. WALZ. Because I think the public sees this and they said encrypt the dang things and do not let anybody get in and do not have default passwords and everything will be fixed.

What I am hearing, what I am feeling is that is not enough, that there still needs to be this credentialing, there still needs to be a culture shift on data security. And we need to make sure that access to the right information to the right people is still granted. Is that true?

Ms. FINN. Yes, sir. I would agree. The biggest vulnerability I think for data is at the end user, you know, the laptop that is not encrypted. And as you said, it is easy to have 26 million records or data about individuals' privacy information.

Mr. WALZ. And, again, I appreciate all the work you are doing and all the folks that are here.

I yield back, Mr. Chairman.

Mr. MITCHELL. Thank you.

Mr. Buyer.

Mr. BUYER. Thank you very much.

With regard to the security awareness training, where is this type of training done? So, in other words, at a medical center, a new employee comes in, who is responsible for that type of training?

Ms. FINN. In VA for VA employees and I believe contractors also, we take an online course many times. It goes through the principles of information security and awareness and the vulnerabilities.

Mr. BUYER. And who is responsible to ensure that that training actually took place or the person actually did it online?

Ms. FINN. Well, I as the supervisor am responsible for ensuring that the people who work for me take it.

Mr. BUYER. Okay.

Ms. FINN. So for an employee within my own organization, we would monitor it.

Mr. BUYER. Who within a medical center?

Ms. FINN. Ultimately I would assume that it would be the Director of the medical center, through the various departments in the hospital.

Mr. BUYER. Uh-huh. And what role or responsibility would the CIO at the medical center have to ensure that everyone is compliant?

Ms. FINN. I am not certain whether they would receive a report or not. So I think probably VHA would be more able to address that and tell you how that works.

Mr. BUYER. Okay. All right. I am here trying to figure out the best process.

Okay? So, you know, when we talked about the centralizing, the purpose of centralizing and coming up with delineations of responsibilities, you know, I guess I am trying to—I agree with Roger Baker here that if, in fact, if it has the word computer on it, he owns it, you know. And so if, in fact, there is some training out there that is required, even if it comes under VHA, that CIO at

that medical center, it is his business to get in somebody else's business.

So you cannot stovepipe this type of stuff. Would you agree with that? I am trying to figure out, you know, you cannot just say, well, you are a supervisor, you have new employees, you just have to make sure it happens. Okay? Where does the accountability function come in? How do we do the check in the box? I do not want to build bureaucracies here, but I am trying to——

Ms. FINN. Well, I think it is important that accountability is on everybody, that it is not just the CIO's problem.

Mr. BUYER. Okay. It is not happening. You say that in your report.

Ms. FINN. Yes.

Mr. BUYER. So how do we get to there?

Ms. FINN. How do we get to hold everybody accountable?

Mr. BUYER. Yes.

Ms. FINN. That will take a concerted push from all across the organization.

Mr. BUYER. Well, I will tell you what. If we make sure that Roger Baker completely understands that if it deals with computers and it is security awareness and assurances, he owns it.

And if it means that those of whom work for him at the VISNs and at the medical centers, if he has to get a little rough with the Chief Medical Officer or whomever at that medical center, if they are responsible, that is his business.

Is that a good idea to do that or is that a bad idea to do that?

Ms. FINN. I think I will take the high road and say I think it is a very intriguing idea. And I would have to look at the implementation over time to see how that would work out.

Mr. BUYER. Well, I look at, you know, your report. Basically it comes back, sir, and says mixed reviews.

Mr. WILSHUSEN. Right.

Mr. BUYER. So I am trying to figure out if, in fact, we are saying to Roger Baker that you own it, he steps forward and says I accept responsibility, right, well, and then if you have individuals within VHA or in contracting want to go, ooh, not me, you know what, then whom?

And if Roger Baker is going to say it is me, then he is not saying it is just me. He is saying it is my lines of authority. And if, in fact, it is his lines of authority, then sitting at that table when that Director sits at the head of the table and he has all of his staff there, that CIO has to be off the heels and on their toes and in people's business if, in fact, it is a computer system, right? I mean, am I——

Mr. WILSHUSEN. What I would just say is that, you know, certainly the CIO under law, and this is including FISMA's responsibilities that it assigns to specific individuals, to the head of the Agency, to senior agency program managers as well, as well as the CIO, senior agency program officials also have responsibilities to ensure that security is appropriately implemented within their sphere of influence and over the IT resources supporting their program.

The CIO, of course, is responsible for implementing the different aspects of an agency-wide information security program, which in-

cludes computer security and awareness training. And the CIO is also supposed to assist and help assure that the senior program managers are performing their responsibilities.

So I would just submit that it is important for the CIO and those individuals that are responsible for ensuring that information security activities such as providing computer security awareness training to their employees are held accountable to assure that they, in fact, do that. One way to do that is to make that part of their performance appraisal system.

Mr. BUYER. Bingo.

Mr. WILSHUSEN. Is it part of the responsibilities of those individuals and are they being held accountable?

Mr. BUYER. We talked about that 4 years ago.

Mr. WILSHUSEN. That is exactly right.

Mr. BUYER. Okay?

Mr. WILSHUSEN. And we made that recommendation——

Mr. BUYER. I remember this conversation.

Mr. WILSHUSEN [continuing]. In the 2007 report. You know, to the extent that VA has implemented that particular aspect of that is one of the things we will be following up this year.

Mr. BUYER. Mr. Chairman and to the Ranking Member here, that is an extremely important thing. I mean, that is something we do not have to legislate, you know. The Executive Branch can actually put this in. And I will be interested when the VHA comes up and testifies. We can ask them.

We should not be handing out bonuses, right, you know, to individuals of whom are not in compliance with the law? And if we actually put it in their performance reviews or it is one of their line items, right, and they have not, then guess what, you get dinged. I mean, boy, you can get somebody's attention pretty quick, you know, and we do not have to legislate that. I mean, the Executive Branch can lean forward on it.

And your point is very well taken. We have talked about that. I really do not know what has happened over the last few years with regard to that particular issue.

But I yield back. Thank you.

Mr. MITCHELL. Thank you.

Dr. Roe.

Mr. ROE. Just one brief comment. What the Ranking Member is stating I think very clearly is those of us who have been in the military understand the chain of command. If you have two silver bars, the guy with one silver bar will say, yes, sir, no, sir, yes, ma'am, no, ma'am. We understand that. We get it. And so it is the chain of command.

And my question, Mr. Chairman, is in the testimony here is in addition, Congress enacted the Veterans Benefit Health care and Information Technology Act of 2006 after a serious loss of data earlier that year revealed a weakness in the VA's handling of personal information.

Under the Act, VA's Chief Information Officer is responsible for establishing, maintaining, monitoring Department-wide information security policies, procedures, control techniques, training and inspection requirements as elements of the Department's information security program. And that is very clear to me. Whoever that

person is, whatever that name is, they are the ones. The buck stops on their desk. And, I mean, it seems very clear to me that that is what you do.

And I agree with you 100 percent that we should not be handing out bonuses. It is clearly stated right here in your testimony where this responsibility is.

And I guess my question is, why did it happen?

I yield back.

Mr. BUYER. Would the gentlemen, would you yield to me for a second?

Mr. ROE. I will.

I will yield, Mr. Chairman.

Mr. BUYER. When we designed this system, the reason that we sort of took the CIO and said, okay, we have them at the top and we are going to take the CIO out of this direct—actually, we did a direct chain of responsibility and authorities.

I did not want a Medical Director to sit there when the CIO gives some push back to that CIO to be big-footed, you know. If there is a real serious concern, I do not want the Medical Director to big-foot him. That CIO works for the VISN CIO and works directly for Roger Baker. So we designed that system. It is sort of like the OIG being outside the system for the accountability function.

And that is why I guess I am leaning right now on saying I think it is a good thing the way we have designed this system for that CIO at the medical center to get in people's business. I mean, it is his job. That is the reason we designed it that way.

And you know what? It does not make them very popular at the table. But, you know, they just have to do that. And we designed it to be like that.

I yield back.

Mr. ROE. I yield back.

Mr. MITCHELL. Thank you.

And I want to thank the panel this morning and appreciate your service very much as all of us do in this Committee. Thank you.

I would like to welcome panel two to the witness table. And for our second panel, we will hear from the Honorable Roger Baker, Assistant Secretary for Information and Technology and Chief Information Officer, U.S. Department of Veterans Affairs.

Mr. Baker is accompanied by Jaren Doherty, Acting Deputy Assistant Secretary of Information Protection and Risk Management, Office of Information and Technology (OI&T); Jan Frye, Deputy Assistant Secretary for Acquisition and Logistics; and Fred Downs, Jr., Chief Procurement and Clinical Logistics Officer for the Veterans Health Administration.

And I would like to recognize Mr. Baker up to 5 minutes. And, please, keep your testimony within 5 minutes because your whole testimony will be part of the record.

Mr. BAKER. Thank you, Mr. Chairman.

Mr. MITCHELL. Thank you.

STATEMENT OF HON. ROGER W. BAKER, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND CHIEF INFORMATION OFFICER, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY JAREN DOHERTY, ACTING DEPUTY ASSISTANT SECRETARY FOR INFORMATION PROTECTION AND RISK MANAGEMENT, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; JAN R. FRYE, DEPUTY ASSISTANT SECRETARY FOR ACQUISITION AND LOGISTICS, OFFICE OF ACQUISITION, LOGISTICS, AND CONSTRUCTION, U.S. DEPARTMENT OF VETERANS AFFAIRS; FREDERICK DOWNS, JR., CHIEF PROCUREMENT AND CLINICAL LOGISTICS OFFICER, VETERANS HEALTH ADMINISTRATION, U.S. DEPARTMENT OF VETERANS AFFAIRS

Mr. BAKER. Ranking Member Buyer, Ranking Member Roe, Members of the Committee, thanks for the invitation to talk about FISMA. Thank you for introducing the folks that are with me today.

And rather than recapping my written testimony, given Congressman Buyer's letter to Secretary Shinseki this past week and the addition of Mr. Downs and Mr. Frye to the panel, I would like to use my time for my oral testimony to recap some of the changes being made at VA in the information protection area.

Last year, I tasked my Information Protection and Operations staffs with implementing technologies that would provide our Central Network Security Operation Center with visibility to every device on our network. Currently our plan calls for this work to be completed by September 30th of this year.

This visibility is essential to allow us to ensure that our policies are being followed throughout the enterprise and monitored, that unauthorized devices are not allowed to connect to the VA network, that all non-medical data devices are encrypted, that all VA systems have intrusion protection software operational, that all VA systems are configured to prevent non-encrypted memory sticks, and that all devices have had the latest patches applied.

This capability will address a large portion of the outstanding recommendations from our FISMA audits, help us better protect our networks and information. It will bring us further along the path towards our goal of being among the best organizations public or private in information protection.

As recent events have shown, however, we cannot be satisfied with protecting veterans' personal information just on the VA network and VA-owned devices. Providing care and benefits for our veterans requires that VA partner with over 22,000 private sector companies across the United States to form our complete supply chain and that we share information with them that will allow us to help provide those services.

Our policy which is stronger than any similar sized private sector organization that I am aware of is that these supply chain partners must follow VA's information protection policies including encryption of mobile devices.

Each contract we sign with a supply chain partner that involves information exchange must contain a clause requiring their adherence to VA Directive 6500.

As you are aware, a laptop computer containing the unencrypted information from over 600 veterans was stolen from the automobile of a VA partner company employee on April 22nd of this year. This information was not encrypted despite the fact that contracts with the company included the required security clause and that the company had certified to the VA that they were in compliance with the clause.

While VA is conducting a formal root cause analysis to determine all the changes that we need to make, we have immediately implemented several changes to address weaknesses in our execution identified by this event.

First, at the request of Mr. Downs and VHA, staff from the Office of IT Oversight and Compliance (ITOC) within my organization will deploy to selected sites to review all contracts and ensure that the necessary contract clause for information security has been included in all contracts where information is exchanged.

I would note the way we selected those sites is they are the ones that did not have the clause with that particular vendor. So they kind of self-selected.

I am explaining the purview of my information security officers at each site to include the review of all contracts where any information is exchanged. Previously their scope had been limited to IT contracts.

I have instructed my IT Oversight and Compliance leadership to include a review of all contracts again where information is exchanged as part of the information security audit they perform at each VA facility. As with the Information Security Officers (ISOs), this had been previously limited to IT contracts.

And as part of their review, the ITOC folks will also randomly select a number of contracts at each facility for a more in-depth audit of that partner's compliance with VA's security policies including on-site inspections.

These steps put VA in an unprecedented position of auditing our supply chain partners to ensure compliance with our information protection policies. While it is impossible to audit all of our partners, these steps should provide us with substantially improved insight into the level of protection provided to veterans' personal information anywhere it exists in our extended enterprise.

Even when we achieve our overall information security goal of being comparable to the best private sector organizations, data breaches will remain an unfortunate fact of life.

Today the majority of data breach incidents we report to this Committee on a monthly basis are paper, not electronic in nature. For that reason, we have established a data breach handling process and office that I believe are among the best, if not the best in the country.

We have established mandatory annual security and privacy training for all VA employees and we have installed information security and privacy officers at each of our facilities to ensure a local focus on those issues.

We are working to establish a culture that encourages everyone to come forward when a data breach is suspected so that it can be quickly and effectively dealt with.

We recognize that we are far from perfect and that we have a long way to go to achieve our information protection goals. But I hope this Committee will recognize the work of the many VA employees and contractors, people of good will and earnest effort, who have already brought about a substantial improvement to our information protection capabilities.

I thank the Committee for your long-term support and your long-term attention to these issues. And my colleagues and I look forward to your questions. Thank you.

[The prepared statement of Mr. Baker appears on p. 43.]

Mr. MITCHELL. Thank you, Mr. Baker.

And I do recognize and I think everyone here recognizes the hard work that the VA employees are doing.

A couple quick questions. In fiscal year 2009, the VA had the lowest of any reporting agencies of government log-in users who are trained on information security awareness.

And what is the reason for this low number?

Mr. BAKER. Congressman, I am better prepared to speak to where we are today than——

Mr. MITCHELL. Okay, sure.

Mr. BAKER [continuing]. That number. But we can go forth on numbers.

Mr. MITCHELL. Right.

Mr. BAKER. One of the reasons that I understand is that in the past we had not removed contractors from the database that were no longer contractors at the company or at the organization and so they would remain in those that looked like they needed training and they were not available to take the training.

But rather than go through those, let me tell you where we were as of yesterday.

Mr. MITCHELL. Okay.

Mr. BAKER. Of the 453,000 people that we viewed as needing to take the security training, we had a compliance certificate for 413,389 of them. That is roughly 91 percent. On privacy training, of the 417,000 we viewed as needing to have a certificate, we had 375,000 that were viewed as compliant or about 90 percent.

Those are the numbers that I was provided when I asked yesterday. As was pointed out, we have an automated database for tracking all this. Our learning management system is where all this training is done, so we are able to keep track of who takes the training.

In particular, a discussion that we are having right now is with all of the new school folks, all the new trainees coming through, roughly 100,000. How will they be quickly trained including mandatory security and privacy training and ensure that they are in compliance as they come through the door?

And my understanding is that over the next couple of months, we will bring about 100,000 of those folks into the VA. They have to take that training before they are allowed on the VA systems. And we are currently working that particular issue.

So I think our numbers have gone up by what I am seeing.

Mr. MITCHELL. And along the same line, I do not want to go back to see where we are from today. The Federal Desktop Core Con-

figuration, FDCC, said that in the past, the VA ranked very low, 22 out of 24.

Can you explain why the VA only had between 26 and 35 percent of its workstations and laptops in compliance? I assume that is past also and that you are also abating that?

Mr. BAKER. I know that number has gone up. A lot of that has been affected by the fact that with our desktop lease, we have been replacing old desktop systems with newer ones that can meet the core configuration.

There are a couple of systemic things that we do have. We have a number of applications that are critical to us that have to be granted waivers. I believe that is viewed as being in compliance with the waiver, but the waiver has to be granted.

And let me ask Mr. Doherty if he has any comments further from that standpoint.

Mr. DOHERTY. We have actually spent the last year and a half going through FDCC in detail. We have granted over 30 waivers. And what a waiver is is it changes the FDCC compliance requirement at the National Institute of Science and Technology so that it will not break any of our applications or disrupt any of our processes.

We are currently at about 70 percent of all of our workstations implemented and we are implementing the FDCC as part of the desktop replacement. And that should be completely finished by the end of next fiscal year.

Mr. MITCHELL. Very good.

Dr. Roe.

Mr. ROE. Just a couple.

First of all, Mr. Baker, you have an enormous job in front of you. My hat is off to you for that, to make sure you have security on how many 10s of thousands of computers there must be in the system.

Mr. BAKER. About 450,000.

Mr. ROE. Four hundred and fifty thousand, wow.

I know that my experience with an electronic medical record is in our own practice with 350 employees involved, we, to my knowledge, so far in 3 years of that system, we have not had any security breaches. And basically we are very careful about who gets in. And everyone is trained.

I think the training is absolutely paramount and to emphasize to people how important this is, that now with the capacity of people outside the site to hack and get in, that information of veterans which should be no one's but the veteran's personal information should be shared with anyone.

I want to make sure I understood this. By September of 2010, that is only about 90 days from now——

Mr. BAKER. That is right.

Mr. ROE [continuing]. All this is supposed to be taken care of? I mean, we are going to——

Mr. BAKER. I would not go so far as to say it will all be taken care of. Visibility to the desktop will provide us with the ability to monitor a number of things that we have had to trust to this point.

I frequently use the Ronald Reagan phrase of trust but verify at this point. We will have electronic access to review every desktop

on the network and verify that they are in compliance with the things that we believe they should be in compliance with.

So I think it gives us a much greater belief that, for example, their patching levels are at the right level. They are not going to get viruses they should not get, that they are configured in such a way that unauthorized devices cannot come into the network, and we have had issues with that in the past, that those devices that are supposed to be encrypted are, in fact, encrypted. So it is a level of confidence that no CIO at VA has ever been able to provide before.

I know I testified in front of this Committee a few months ago and was asked I believe by Congressman Buyer that question. If I am going to provide you with a certain statement, you know, we are in high 90s compliance, then I am going to do that when I have not just people throughout the organization reporting that to me on paper, but when I have an organization that can look at those devices and say we are in 99.95 percent compliance on this issue. And that is where we are going by the September 30th date.

Mr. ROE. Well, that is impressive. I think the thing that just me sitting here now a year and a half is that, you know, we had the, and this has nothing to do with you, but the Vision Center of Excellence which a year ago in March, I think we had our first hearing and we are now a year later and I cannot tell it has moved off the mark very much.

And I know we were told that DoD and VA at Great Lakes were going to be able to interface and all that by this fall and now it probably will not happen.

So I really believe the security breach is one of the most important issues that we face because of identity theft that is going on in the country now.

I know that my wife used a credit card here in Washington, DC, on her last visit and because that was out of the ordinary, when I went home to use it, you could not use it. I mean, they were very careful about how they—and I appreciate that as a consumer.

And as a veteran, I appreciate the VA's best effort at being able to make sure that we do not lose valuable data from veterans that have served.

I yield back my time.

Mr. MITCHELL. Thank you.

I will let Mr. Zach Space get a little oriented here and I will ask Mr. Buyer if he would like to go. Well, he just walked in, so let him get settled here. Go ahead.

Mr. BUYER. Okay. Thank you.

Mr. Baker, you were sitting here when I had a discussion with the first panel and, you know, the reaction from the OIG with regard to who, I am sort of paraphrasing this now, but who is going to be responsible for the protection of certain information. Obviously their reaction was that the supervisor, direct supervisor. Well, I will agree.

But as soon as that information ends up in the IT environment, does it not change? I am going to throw that now to you.

Mr. BAKER. Yes. I believe at this point, and I will freely admit that this incident has caused us to look at the scope of control that IT has taken on these things, but recognizing that, we have recog-

nized that we need to accept responsibility for protecting veterans' information wherever it exists in our very extended supply chain as the VA.

And that means going beyond writing the policy which has been the primary role of IT, you know, from the past and into looking at everywhere it is going, not just in the IT systems of the VA, but throughout all of our partners and their IT systems.

I would also point out, to make this point again, paper is becoming even more interesting than electronic for us. There are a lot of things we can do to lock down our electronic systems.

I agree with Congressman Roe's point that paper is slower, but paper is also harder to detect from an information breach standpoint. And so it is an interesting point.

Back to your point, yes, we have extended the controls at this point and we will take that responsibility.

Mr. BUYER. Secretary Frye, you oversee VHA contracting, correct?

Mr. FRYE. I do not oversee VHA——

Mr. BUYER. You do not?

Mr. FRYE. No, I do not oversee VHA contracting. We have a decentralized system across the VA and VHA has their own authority to let contracts and administer those contracts.

Mr. BUYER. Okay. So I should ask this question of Mr. Downs. Is that what you are doing? You are kicking the guy to——

Mr. FRYE. No, I am not, sir. I write policy.

Mr. BUYER. Well, let me ask—pardon?

Mr. FRYE. I write policy. I am responsible for formulation and promulgation of policy across the VA. But I do not own the contracts per se for VHA. That is the point I am trying to get across.

Mr. BUYER. And the point I am about to try to get across is you should. I dislike the decentralized process. I dislike it. I detest it. And I would prefer to have testimony by someone that would say I own it, not just I give policy. I would love to be able to change the law that says he owns it. I detest, I am going to repeat, I detest this decentralized model.

When we move into our procurement reform, Mr. Chairman, I am hopeful that we can work together to move to more centralization.

Now, the contractor in question that experienced a stolen, unencrypted laptop had 69 contracts involving 13 VISNs and 30 VA medical centers. Each of these contracts were separately negotiated and 25 lacking the required security clauses. This is not a good example of a decentralized contracting system.

Now, Mr. Downs, you are the Chief Procurement Officer for VHA, correct?

Mr. DOWNS. That is correct.

Mr. BUYER. Now, can you tell us what your responsibilities are with respect to contracting and the procurement process in VHA?

Mr. DOWNS. Yes, sir. I am the Chief Procurement and Logistics Officer for VHA. And my job is to oversee the complete supply chain within VHA, logistics, the acquisition, procurement, and prosthetics, which all go to support the medical care system.

And I have a Deputy in each one of those positions, procurement, logistics, and prosthetics. They are the ones then who are respon-

sible for making sure that the policies are carried out within VHA at all levels.

And in the procurement area, we have centralized all of those contracting officers to my direct chain of command. We will finish that with all the other purchasing elements in VHA by the end of this fiscal year.

Mr. BUYER. However we are going to do this, Mr. Chairman, we have got Secretary Frye. He is sitting in the Central Office. He is the guy that directly responds to the Secretary. And I am trying to figure out how we link this so we have better command and control. I am not there yet. I am looking for ideas on how best to do this as we move forward with our legislation.

The Acquisition Service Center in VISN 9 at Murfreesboro, Tennessee, comes directly under you; does it not, Mr. Downs?

Mr. DOWNS. Yes.

Mr. BUYER. So now that you said that you are centralizing, these contracting officers then, do they work for you?

Mr. DOWNS. Yes, they do work through the chain of command. The way I have set it up, we have the Deputy Procurement Officer and then we have set up three service area officers divided so we have span of control. And within that one is a Central SAO, Central Area Officer. And so those contracting officers and——

Mr. BUYER. So are the contracts then that are let at the Acquisition Service Center then reviewed at a higher level?

Mr. DOWNS. Yes, sir.

Mr. BUYER. Okay. When they are reviewed at a higher level, I mean, obviously they know now about the security clauses that are required, but for whatever reason, that was not picked up, right? Contracts were being let without that and we are having to go back in and do the modifications?

Mr. DOWNS. In some cases. But, again, it is a question of what type of contract was it. When we went through our review last year of the 23,000 contracts and there were 6,000 contracts that did not have the security clause that we felt needed to be inserted, we asked for certification that that be done.

And the certification came to us last year and said that those they believed needed the IC or the security clause had been added. There were questions on some others. There were 578 where the vendor refused or did not believe that they had to sign that clause or have it assigned to them.

So we then went into a mode where we had to look and see, well, what is the reason behind that, is it valid. And not all were required to have that clause. The remaining contracts of this 578 were critical to our medical centers' ability to provide patient care.

And they are either for the direct health care services with our nursing homes, our hospice physicians, academic affiliations, or in direct support of our health care maintenance on medical equipment for MRIs, CT scanners, for instance.

And we had to weigh that because the risk of not having the contracts was high and the guidance was simply not clear on the applicability of the clause to health care contracts. That was hard for people to figure out, particularly where those medical doctors were covered by the Health Insurance Portability and Accountability Act or where the VA did not own the data.

So we consulted with legal, privacy, and the ISOs and the consensus was VA Handbook 65 was being revised to clarify the clause. And so we are waiting for that to occur.

Mr. BUYER. Do you own compliance responsibility?

Mr. DOWNS. Excuse me, sir?

Mr. BUYER. Do you own compliance responsibility?

Mr. DOWNS. Yes, within VHA.

Mr. BUYER. You do? What are the consequences for a contractor's false certificate of compliance?

Mr. DOWNS. When a contractor has——

Mr. BUYER. Yes.

Mr. DOWNS [continuing]. False compliance, then I would have to work with General Counsel to determine what, after due process, what had to be done.

Mr. BUYER. And what actions have you taken against those contractors out there that have false certificates?

Mr. DOWNS. Well, on this recent occurrence, we have issued a—the show cause letters have gone out to all of those 55 contracts with this particular vendor. And when we get results back from the show cause, we will then meet with the Office of Acquisition and Logistics (OAL) and we will meet with the General Counsel.

Mr. BUYER. At what point in this process do you communicate with Roger Baker? If you are saying, okay, I have responsibility with compliance, he has some overlying responsibility, too, because he is looking to make sure that things are going to be taking place, how do you two communicate?

Mr. DOWNS. Absolutely. We talk on a regular basis as far as that goes. But this particular issue here was a security clause. We have looked at what we have to do to strengthen our ability to ensure that IT clause is in there, clarify it. So he has initiated an audit process, which I will let him discuss. So his folks will be reviewing the contracts.

We have sent orders out to our contracting officers that on every contract that they suspect or even close to being either IT security or patient information sensitive, they will meet with the ISO and have a discussion as to whether this particular contract does need that clause or not.

Mr. BUYER. May I ask one more?

All right. You have articulated very well with regard to teams that you have put together with regard to this issue on compliance and the medical services provided is, quote, so important.

So much of our medical technology also incorporates IT. Okay? So some of the radiological systems that you have also mentioned is IT.

I am trying to figure out here, Mr. Chairman, how are we going to ensure compliance. I mean, if we have a contractor out there that is saying I am not going to sign your mod, you are doing some contracting for maybe a radiological service out there and they are saying we are not going to sign.

You have a CIO sitting at the medical center that says to the Medical Director, you are not in compliance. How do we resolve this? Seriously, gentlemen. How do you resolve that? How do you do that?

Mr. BAKER. If I could, that is the challenge at large across the organization with this information. The primary purpose for the information is to provide care to veterans. We have to protect that information from unwanted access at the same time that we provide it to anyone who wants to do it.

You touched on the point of medical devices which adds another layer of complexity because many of the medical devices are certified by the Food and Drug Administration (FDA) in a particular configuration to operate a certain way.

Mr. BUYER. Medical devices meaning medical technology?

Mr. BAKER. Medical technology. We have to be very careful from an IT perspective how we interact with the medical technology.

For example, we cannot apply patches to that technology because it could have unknown effects on the performance of, say, an MRI machine or something along those lines. It adds another level of complexity and it is something that I believe VHA is tackling in advance of the rest of the country.

You know, we see it. We are working together on it. But to that point, it is a mutual. It is IT and it is medical and it exemplifies the whole discussion around VHA and OI&T related to information. How do we do great medical care and protect the information at the same time?

Mr. BUYER. I do not know. Seriously, I do not know and that is why we are going to lean to you to do that because you have to safeguard. You are the guardian, right? Both of you, you are the guardian of that. I am going right at you, Mr. Chairman. You are the policy guy.

Mr. FRYE. Yes. Mr. Buyer, there is a methodology where we would unilaterally apply the security clause to a contract, whether the contractor likes it or not, and he can come back to us under the changes clause and protest that perhaps and attempt to charge us for insertion of that clause. We were very clear, I believe, on our instructions to the contracting officers to do that.

Now, I think the 570 some contracts that Mr. Downs talked about had other issues, at least based on what I have been told. In some cases, for instance, under fee basis, the physicians that a veteran would see are not under contract. And so the fee-basis provider owns that information. The VA does not. There is no contract in place. So we would not put a clause in any contract because there is no contract.

So that is an issue that Mr. Downs has been working with General Counsel. But clearly if we have a contractor that is recalcitrant, who refuses to accept the clause, we can either terminate the contract or we can unilaterally apply it and let them come back to us under the changes clause.

Mr. BUYER. Thank you, Mr. Chairman.

Mr. MITCHELL. Thank you.

Just to kind of follow-up, why do you not just put the security clause in every contract and let them, as you said, challenge it?

Mr. FRYE. That is a good question, Mr. Chairman. Here is what we did. In November of 2008, we put the security clause in our electronic contract writing system so that every contract that is now written in the VA has that clause in it. The only way it can be removed is by a conscious decision by a Contracting Officer. So

they have to take a positive step to remove it from any contract they develop.

The contracts we are talking about are those contracts that were let before November of 2008. There was a decision made by Mr. Baker's predecessor not to include that clause, the security clause, in any contracts that were let prior to November of 2008.

When our new Secretary came on board, Secretary Shinseki said, hey, we have some risk here and working with Mr. Baker, they decided to go back retroactively and apply this clause to those contracts that did not have them.

So, in fact, we looked at nearly 30,000 contracts and 22,700 of those were in VHA. The rest of them were in organizations that fall under my purview.

Mr. MITCHELL. Let me just ask one quick question. Are these contracts for life?

Mr. FRYE. No, sir.

Mr. MITCHELL. How often do you renegotiate them?

Mr. FRYE. Normally when we put contracts in place, we put a contract in place with a base year and option years. And those option years usually consist of 4 years so that we get a total of 5 years out of a contract if we decide to exercise those options. Yeah. The base lasts for 1 year and the clause that we put in the contract lasts for the entire life of the contract if we exercise the options.

Mr. MITCHELL. Thank you.

Mr. Space.

Mr. SPACE. Thank you, Mr. Chairman.

Just as a follow-up, if you know, why would Assistant Secretary Baker's predecessor determine to take out the security provisions from the contract?

Mr. BAKER. I do not think it was a taking out. I think it was which contracts does it apply to effective today. And the decision was made that it would apply to all new and that at that point, they would not go back and look retroactively.

I would tell you that, I think the culture at VA has changed incredibly under the new Administration, under Secretary Shinseki. It is a much more cooperative arrangement between OI&T and VA. And it is very clear that we will continue to operate that way while Secretary Shinseki is on the 10th floor.

I think I probably have more ability to work with VHA and encourage them to look at things a certain way than my predecessor did.

Mr. SPACE. Great. And I certainly want to agree with you that General Secretary Shinseki has, I think, begun to change the culture at the VA in a very positive way. But I have to tell you I am a little bit disturbed by how some of these breaches were handled and I will explain if you will allow me.

I have a copy of the letter that was sent to those veterans whose identities or personal information have been compromised as the result of either the theft of the laptop or the loss of the binder in Texas.

And in that letter, first of all, it is from the Veterans Health Administration and not from the VA. I just really felt that this was such an important issue that perhaps some, and this is meant as no disrespect to Mr. Downs at all, but I felt that this was such that

perhaps it should have gone higher up the chain in terms of creating the illusion of importance which it is very important.

Also, you know, if you read the language in the letter, it seems to implicitly put blame on a contractor. It refers to a Heritage provided unencrypted laptop.

And, you know, one of the things that I really feel very strongly about and I think that one of the things about the VA culture that Secretary Shinseki has been working very effectively on is understanding that at times, you have to stand up and accept responsibility when a mistake has been made.

When that happens, the likelihood of that mistake being repeated goes down dramatically. And for what it is worth, you know, I would have liked to have seen maybe a more honest or open expression of the circumstances surrounding the security lapse.

And I guess along those same lines, apart from this letter, was there any other effort made to notify those veterans whose identity or private information may have been compromised?

Mr. BAKER. The letter is the primary notification to the veteran. We take a lot of care in finding an address for those veterans, recreating what information was there and making certain that we know which veterans to notify.

We have not yet determined if we will put out a what in this case would be a national press release on this. This is an interesting breach because of the way it, if you will, impacts with the High Tech Act. The recent implementation of the High Tech Act says that over 500 people in a jurisdiction triggers an automatic press release in that jurisdiction.

Mr. SPACE. Uh-huh.

Mr. BAKER. In this case, there were 10s of people in each of a variety of jurisdictions. So while legally in the reading of the High Tech Act the advice we have gotten is, well, legally it does not trigger it. We have not made a management decision as to whether we will press release at this point.

Mr. SPACE. Yeah. And that is a decision that you will have to make, but it would seem to me that issuing a press release would certainly be in compliance with the spirit of those provisions.

I know that from the information I have that approximately 3,200 veterans had their personal information exposed, but my understanding is that is the result of the loss or theft of a binder and clipboard on April 24th. Is that a correct figure?

Mr. BAKER. I do not know the date specifically, but that is basically correct, yes.

Mr. SPACE. Do we know how many veterans may have had their personal information exposed as a result of the laptop theft?

Mr. BAKER. It was just over 600.

Mr. SPACE. Okay.

Mr. BAKER. Do we know the exact? Six forty-four, I think, is the right number.

Mr. SPACE. And there has been no effort to reach out personally to these veterans on the telephone or via anything other than a letter?

Mr. BAKER. Beyond a letter, I am not aware of anything further done, no.

Mr. SPACE. Okay. All right. Thank you, Mr. Baker.

I yield back.

Mr. MITCHELL. Thank you.

Mr. Buyer.

Mr. BUYER. I have a liability question. Secretary Frye, with regard to your policy and you have a contractor of whom is now responsible for a breach, what is the policy with regard to going back against the contractor for the cost that we have now incurred with regard to notification and credit monitoring?

Mr. FRYE. That is a very important question. We do have recourse against the contractor. First of all, we could terminate the contractor for default. And we may do that in this case. As Mr. Downs has said, we have already issued show cause letters.

Second, we are going to take some action against them with regards to past performance and enter that into the database that is used nationally to talk about past performance to other contracting officers when they attempt to let a contract.

Thirdly, we have remedies in court. And, of course, I do not get involved with those. We let counsel take care of those. But there are remedies in court in case we suffer damage that requires us to take them to Federal Court.

Mr. BUYER. Thank you.

Mr. Downs, then you are going to take the position then, you issue your show cause letters and you are going to go after these contractors to recoup the costs? Is that what you are attempting to do?

Mr. DOWNS. When the response comes back from the show cause, we will sit down with General Counsel because we will have to follow their guidance on what is best to do. And, of course OAL is involved with that. Mr. Frye's office and Mr. Baker's office will be involved with that because this is a team effort as we try to work our way through this so that we are able to make corrections and ensure that it does not happen in the future and, if so, then what is our best course of how we would address it. But, yes, sir.

Mr. BUYER. Mr. Chairman, not only are we put on notice with regard to these contractors, but we are willing to hold them responsible and recoup the costs where they are going to participate with the compliance on security assurances.

I yield back. Thank you.

Mr. BAKER. Sir, if I could just make one point to the credit of the contractor. They self-reported this and they have been very cooperative from the point forward. It does not mitigate what they did not do right, but since their name has come out, I do want to point out that they have been very helpful in identifying, for example, who were the veterans who needed to receive the letter.

You know, if you look at the timeline on this, they notified VA very quickly. And as we build that culture, it is important that we encourage people to report because we cannot mitigate the issue unless we know about it.

So having said that, to Congressman Space's point, having in essence said the contractor is responsible, VA also is responsible. We need to make certain that our culture allows them to report and encourages that type of approach to things.

So thank you.

Mr. MITCHELL. Thank you.

You know, it is one thing to have hearings like this to try to find out what is going on, but we would like to have you follow-up at least by September of where you are on all of this, the progress you are trying to make, and give us a report back the status of your work.

Mr. BAKER. Sir, given the date for this is supposed to be September 30th, would October 15th be an adequate date?

Mr. MITCHELL. That would be fine.

Mr. BAKER. Great.

Mr. MITCHELL. Thank you.

I want to thank all of you for your service to this country as well as to the veterans of this country. And we appreciate everything you are doing and keep up the good work.

Thank you.

Mr. BAKER. Thank you.

[Whereupon, at 11:40 a.m., the Subcommittee was adjourned.]

A P P E N D I X

Prepared Statement of Hon. Harry E. Mitchell, Chairman, Subcommittee on Oversight and Investigations

Thank you to everyone for attending today's Oversight and Investigations Subcommittee hearing entitled, *Assessing Information Security at the U.S. Department of Veterans Affairs.*

Today, we will examine the current status of information security at the VA and its ability to protect itself against both malicious and accidental sensitive information breaches. The Department of Veterans Affairs employs its sophisticated computing infrastructure to store the health and financial records of millions of American veterans and their families. Each day, there is the potential for millions of attempts to gain unauthorized access to government computers that hold this information through unsecure ports and other means.

The risks to the VA of not implementing a sound information security program are considerable, and unfortunately, have already been seen through several situations in the past. Just recently, we have learned of two data breaches: In Texas, 3,265 veteran's records were compromised when information went missing from a facility conducting lab tests. In a second instance in Texas, a VA contracted company had a laptop stolen compromising the records of 644 veterans. These recent data breaches are proof that the VA still has a long ways to go in ensuring our Nation's veterans that their most sensitive information is being safely stored and handled.

The Federal Information Security Management Act of 2002 or FISMA is a critical and evolving mandate designed to help Federal Government entities, including the VA, protect personally identifiable and otherwise sensitive information. In March of this year, the Office of Management and Budget (OMB) released its FY 2009 report on FISMA. Unfortunately, the VA ranked *dead* last among other FISMA monitored agencies in areas such as the percent of log-in users trained on information security awareness, and also in the issuance of personal identity verification. Additionally, the OMB report also lists the VA as one of 6 federal agencies identified as having a material weakness.

It is clear that the VA has a wide range of areas in which it must improve its information security infrastructure. Strengthening interagency network connections, access controls, and improving configuration management are some of the things that will yield positive results in securing VA's computing network. In light of the recent data breaches in Texas and OMB's recent release of its FY 2009 FISMA report, there is no better time to review VA's information security posture, and hear from the Department how they plan to address the challenges they face in securing the personal information of our Nation's veterans.

I am pleased that both the VA Office of Inspector General and the Government Accountability Office are here to shed light on additional improvements that the VA can make. I look forward to your testimony.

Prepared Statement of Hon David P. Roe, Ranking Republican Member, Subcommittee on Oversight and Investigations

Thank you Mr. Chairman. I appreciate you holding this important hearing.

The security of the information the Federal Government has under its purview is of paramount importance. Recognizing that importance, Congress passed several acts to increase security awareness throughout federal agencies, including the Department of Veterans Affairs. In 2002, Congress passed the Federal Information Security Management Act (FISMA), which permanently reauthorized the framework laid out by previous legislative initiatives such as the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Information Technology Reform Act

of 1996 (Clinger-Cohen), and the Government Information Security Reform Act of 2000. The enactment of FISMA was a critical step to ensure the continuation of requirements and therefore the ability to effectively identify and track the Federal Government's information and system security status.

Prior to 2001, the VA Inspector General (IG) and other outside agencies had expressed concern and identified material weaknesses regarding information security management at VA. Since 2001, IG reviews of VA FISMA compliance continued to identify significant information security vulnerabilities that placed VA at risk of denial of service attacks, disruption of mission-critical systems, and unauthorized access to sensitive data. Numerous security weaknesses were identified, but generally not corrected by VA, even after the IG identified repeat weaknesses over several years. One glaring example of this state of affairs was demonstrated by the FY 2004 report where the IG made 16 recommendations to VA to strengthen information security management, which remained open at least up to May 23, 2006.

Since the data breach of May 2006, the second largest in the Nation and the largest in the Federal Government, we have seen the centralization of VA's information management, including information security. These efforts have continued through the current administration under Assistant Secretary Baker's lead. I appreciate the massive undertaking by both the previous Administration and the current Administration to tighten the controls on protecting the data of our Nation's veterans. However, while progress has been made in centralizing the IT Department at the VA, I am uncertain how much progress has been made in protecting the information managed by the department.

In reviewing the FISMA reports issued by OMB over the past 7 years, I am concerned about VA's status with respect to information security. In May 2006, the VA did not even file a report on its FISMA compliance. In 2007, the VA received an "F" on its FISMA compliance. Most glaring is the recent 2009 FISMA report, which shows that even though VA has over 500 FTE assigned to security-related duties, it has the lowest percentage of log-in users trained in information security (>65 percent), and the lowest percentage of Personal Identity Verification credentials issued by the agency (<5 percent) to employees and contractors.

I am highly concerned that VA is just not taking information security seriously enough. The protection of the personal information of our Nation's veterans should be a high priority at the Department. We do not want another security breach at the Department, and we certainly don't want one that would reach the level of the May 2006 breach. But if VA continues on its current path, we may have just that.

On April 28, 2010, my staff was alerted to a stolen laptop which had access to VA medical center data. This contractor owned laptop was unencrypted, and possibly contained the personal identifying information (PII) of approximately 644 veterans. Upon further investigation, we learned that in November of 2009, the Department issued a directive for VA to incorporate VA Acquisition Regulation (VAAR) clause 852.273–75, which provides for the "Security Requirements for Unclassified Information Technology Resources." VA reviewed 22,729 contracts to determine whether the contracts required the inclusion of this clause—6,440 required the inclusion of VAAR 852.273–75, 5,665 contracts have the clause inserted (88 percent), 578 contractors refused to sign the clause (9 percent) and an additional 197 still require the clause (3.1 percent).

I have many questions over this issue, some of which I hope we can answer in this hearing: (1) Why was the clause not enforced prior to November 2009; (2) Did Heritage Health Solutions have the clause included in their contract; (3) What are VA's plans as far as the 578 contractors who refused to sign the clause when added to their contract; (4) What was the primary reason that most of these contractors refused to sign onto the additional clause; and finally (5) What is VA going to do to tighten the controls on contractor owned equipment that is regularly accessing the VA networks and storing data relating to our Nation's veterans?

To place our veterans information at risk is irresponsible. These men and women have fought for our Nation, have placed their own lives in jeopardy to secure our freedom, and we repay them by tossing caution to the wind with respect to their personal information. This is totally unacceptable. VA must take immediate action to secure our veterans information, and to ensure that all contracts requiring access to any data at the VA include the protections our veterans need and require.

Again, thank you Mr. Chairman, and I yield back my time.

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

INFORMATION SECURITY: Veterans Affairs Needs to Resolve Long-Standing Weaknesses

GAO Highlights

Why GAO Did This Study

Since 1997, GAO has identified information security as a governmentwide high-risk issue. This has been particularly true at the Department of Veterans Affairs (VA), where the department has been challenged in protecting the availability, confidentiality, and integrity of its information and systems. Since the 1990s, GAO has highlighted the challenges the department has faced, including the need to safeguard personal information.

GAO was asked to testify on VA's progress in implementing information security and the department's compliance with the Federal Information Security Management Act of 2002 (FISMA), a comprehensive framework for securing federal information resources. In preparing this testimony, GAO analyzed prior GAO, Office of Management and Budget, VA Office of Inspector General, and VA reports related to the department's information security program.

What GAO Recommends

In previous reports over the past several years, GAO has made numerous recommendations to VA aimed at improving the effectiveness of the department's efforts to strengthen information security practices and toensure that security issues are adequately addressed.

What GAO Found

VA has made limited progress in resolving long-standing deficiencies in securing its information and systems. In September 2007 and also March 2010, GAO reported that VA had begun or had continued work on several initiatives to strengthen information security practices, but that shortcomings in the implementation of those initiatives could limit their effectiveness. VA has also consistently had weaknesses in major information security control areas. As shown in the table below, VA was deficient in each of five major categories of information security controls as defined in the GAO *Federal Information System Controls Audit Manual.*

Security Weaknesses for Fiscal Years 2006–2009

Security Control Area	2006	2007	2008	2009
Access control	•	•	•	•
Configuration management	•	•	•	•
Segregation of duties	•	•	•	•
Contingency planning	•	•	•	•
Security management	•	•	•	•

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

Further, in VA's fiscal year 2009 performance and accountability report, the independent auditor stated that, while VA continued to make progress, IT security and control weaknesses remained pervasive and continued to place VA's program and financial data at risk. The independent auditor also noted that VA's controls over its financial systems constituted a material weakness (a significant deficiency that can result in an undetected material misstatement of the department's financial statements.)

Since 2006, VA's progress in fully implementing the information security program required under FISMA has been mixed. For example, from 2006 to 2009, the department reported a dramatic increase in the percentage of systems for which a contingency plan was tested. However, during the same period, the department reported a decrease in the percentage of employees who had received security awareness training.

Until VA fully and effectively implements a comprehensive information security program and mitigates known security vulnerabilities, its computer systems and sensitive information (including personal information of veterans and their beneficiaries) will remain exposed to an unnecessary and increased risk of unauthorized use, disclosure, tampering, theft, and destruction.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on information security at the Department of Veterans Affairs (VA). Since 1997, we have identified information security as a government wide high-risk issue and emphasized its importance in protecting the availability, confidentiality, and integrity of the information residing on federal information systems.[1] Since the 1990s, we have highlighted challenges the department has faced, including the need to safeguard personal information.

In our testimony today, we will discuss VA's progress in implementing information security and the department's compliance with the Federal Information Security Management Act of 2002 (FISMA).[2] In preparing this testimony, we analyzed prior GAO, Office of Management and Budget (OMB), VA Office of Inspector General (OIG), and VA reports related to the department's information security program for fiscal years 2006 through 2009. We conducted our review from April to May 2010 in the Washington, D.C., area in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

Background

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the Nation by ensuring that they receive medical care, benefits, social support, and memorials. According to recent information from the Department of Veterans Affairs, its employees maintain the largest integrated health care system in the Nation for more than 5.6 million patients, provide compensation and pension benefits for nearly 4 million veterans and beneficiaries, and maintain nearly 3 million gravesites at 163 properties. The use of IT is crucial to the department's ability to provide these benefits and services, but without adequate protections, VA's systems and information are vulnerable to those with malicious intentions who wish to exploit the information.

To help protect against threats to federal systems, FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The framework creates a cycle of risk management activities necessary for an effective security program. In order to ensure the implementation of this framework, FISMA assigns responsibilities to OMB that include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing and approving or disapproving agency information security programs, at least annually. It also assigns specific responsibilities to agency heads, chief information officers, inspectors general, and the National Institute of Standards and Technology (NIST), in particular requiring chief information officers and inspectors general to submit annual reports to OMB.

In addition, Congress enacted the Veterans Benefits, Health Care, and Information Technology Act of 2006,[3] after a serious loss of data earlier that year revealed weaknesses in VA's handling of personal information. Under the act, VA's Chief Information Officer is responsible for establishing, maintaining, and monitoring department wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department's information security program. It also reinforced the need for VA to establish and carry out the responsibilities outlined in FISMA, and included provisions to further protect veterans

---

[1] GAO, *High-Risk Series: An Update,* GAO–09–271 (Washington, D.C.: January 2009) and *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses,* GAO–09–546 (Washington, D.C.: July 17, 2009).

[2] FISMA was enacted as title III, E–Government Act of 2002, Pub. L. No.107–347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

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

and servicemembers from the misuse of their sensitive personal information and to inform Congress regarding security incidents involving the loss of that information.

VA Has Made Limited Progress in Addressing Information Security Weaknesses

For over a decade, VA has faced long-standing information security weaknesses as identified by GAO, the VA's OIG, and by the department itself. These weaknesses have left VA vulnerable to disruptions in critical operations, theft, fraud, and inappropriate disclosure of sensitive information. VA's efforts to address these deficiencies have had limited progress to date.

In September 2007, we reported that VA had begun or had continued several initiatives to strengthen information security practices within the department, but that shortcomings with the implementation of those initiatives could limit their effectiveness.[4] At that time, we made 17 recommendations for improving the department's information security practices. We verified that VA had implemented five of those recommendations, including developing guidance for the information security program and documenting related responsibilities. VA has efforts under way to address 11 of the remaining 12 recommendations. These efforts include ensuring remedial action items are completed in an effective and timely manner, implementing guidance on encryption, and developing and documenting procedures to obtain contact information for individuals whose personal information has been compromised in a security breach. We plan to assess whether the department's actions substantially implement these 11 recommendations, and whether VA is now taking action on the twelfth recommendation to maintain an accurate inventory of all IT equipment that has encryption installed.

In March 2010, we reported[5] that federal agencies, including VA, had made limited progress in implementing the Federal Desktop Core Configuration (FDCC) initiative to standardize settings on workstations.[6] We determined that VA had implemented certain requirements of the initiative, such as documenting deviations from the standardized set of configuration settings for Windows workstations and putting a policy in place to officially approve these deviations. However, VA had not fully implemented several key requirements. For example, the department had not included language in contracts to ensure that new acquisitions address the settings and that products of IT providers operate effectively using them. Additionally, VA had not obtained a NIST-validated tool to monitor implementation of standardized workstation configuration settings. To improve the department's implementation of the initiative, we made four recommendations: (1) complete implementation of VA's baseline set of configuration settings, (2) acquire and deploy a tool to monitor compliance with FDCC, (3) develop, document, and implement a policy to monitor compliance, and (4) ensure that FDCC settings are included in new acquisitions and that products operate effectively using these settings. VA concurred with all of our recommendations and indicated that it plans to implement them by September 2010.

VA Continues to Report Significant Information Security Shortcomings

Information security remains a long-standing challenge for the department. In 2009, for the 13th year in a row, VA's independent auditor reported that inadequate information system controls over financial systems constituted a material weakness.[7] Among 24 major federal agencies, VA was one of six agencies in fiscal year 2009 to report such a material weakness.

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

---

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

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

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

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

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

In addition, VA has consistently had weaknesses in major information security control areas. As shown in table 1, for fiscal years 2006 through 2009, deficiencies were reported in each of the five major categories of information security controls [8] as defined in our *Federal Information System Controls Audit Manual.*[9]

Table 1: Control Weaknesses for Fiscal Years 2006–2009

Security Control Category	2006	2007	2008	2009
Access control	•	•	•	•
Configuration management	•	•	•	•
Segregation of duties	•	•	•	•
Contingency planning	•	•	•	•
Security management	•	•	•	•

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

In fiscal year 2009, for the 10th year in a row, the VA OIG designated VA's information security program and system security controls as a major management challenge for the department. Of 24 major federal agencies, the department was 1 of 20 to have information security designated as a major management challenge. The OIG noted that the department had made progress in implementing components of an agency wide information security program, but nevertheless continued to identify major IT security deficiencies in the annual information security program audits. To assist the department in improving its information security, the OIG made recommendations for strengthening access controls, configuration management, change management, and service continuity. Effective implementation of these recommendations could help VA to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data.

The need to implement effective security is clear given the history of security incidents at the department. VA has reported an increasing number of security incidents and events over the last few years. Each year during fiscal years 2007 through 2009, the department reported a higher number of incidents and the highest number of incidents in comparison to 23 other major federal agencies.

VA's Uneven Implementation of FISMA Limits the Effectiveness of Security Efforts

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

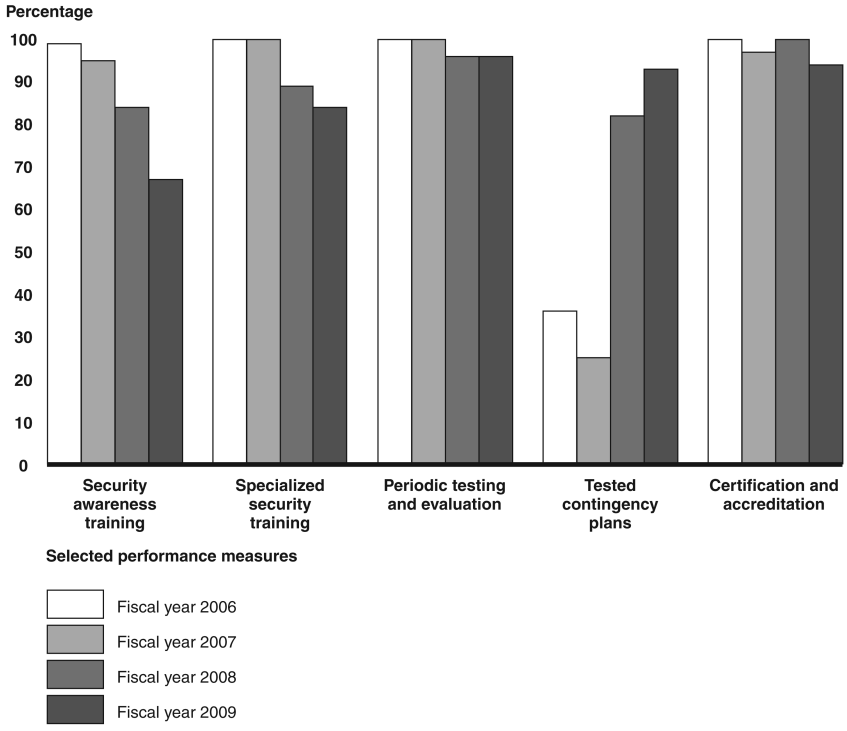
[8] Access controls ensure that only authorized individuals can read, alter, or delete data; configuration management controls provide assurance that only authorized software programs are implemented; segregation of duties reduces the risk that one individual can independently perform inappropriate actions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

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

- employees and contractors receiving IT security awareness training, and those who have significant security responsibilities and have received specialized security training,
- systems whose controls were tested and evaluated, have tested contingency plans, and are certified and accredited.[10]

Since fiscal year 2006, VA's progress in fully implementing the information security program required under FISMA and following the policies issued by OMB has been mixed. For example, from 2006 to 2009, the department has reported a dramatic increase in the percentage of systems for which a contingency plan was tested in accordance with OMB policy. However, during the same period, it reported decreases in both the percentage of employees who had received security awareness training and the percentage of employees with significant security responsibilities who had received specialized security training (see fig. 1). These decreases in the percentage of individuals who had received information security training could limit the ability of VA to effectively implement security measures.

Figure 1: VA Key Performance Measures for Fiscal Years 2006–2009



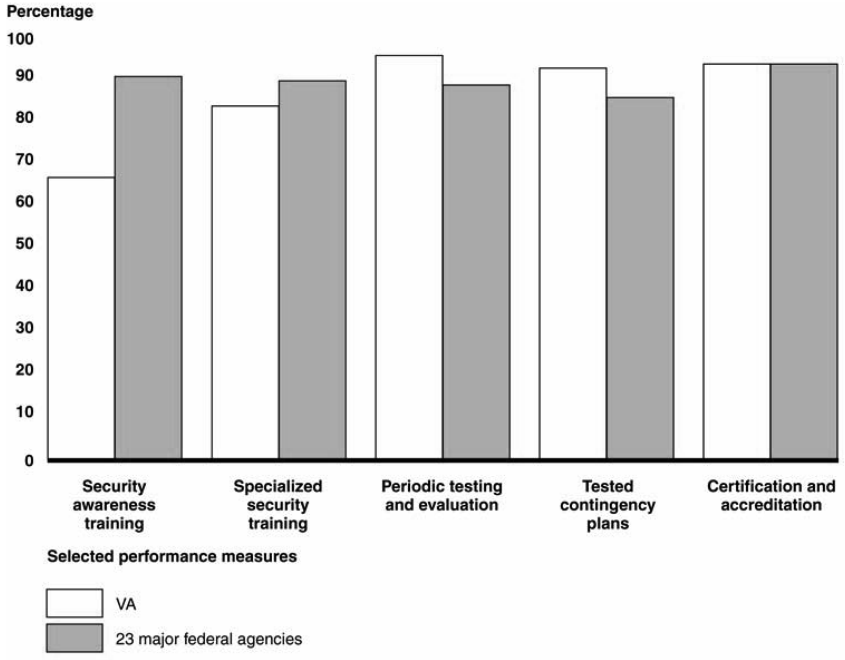
Source: GAO analysis of agency data.

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

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

number of systems that had been certified and accredited. However, VA reported lower percentages of individuals who received security awareness training and lower percentages of individuals with significant security responsibilities who received specialized security training (see fig. 2).

Figure 2: Comparison VA to Governmentwide Performance for Fiscal Year 2009



Source: GAO analysis of agency data.

In summary, effective information security controls are essential to securing the information systems and information on which VA depends to carry out its mission. The department continues to face challenges in resolving long-standing weaknesses in its information security controls and in fully implementing the information security program required under FISMA. Overcoming these challenges will require sustained leadership, management commitment, and effective oversight. Until VA fully and effectively implements a comprehensive information security program and mitigates known security vulnerabilities, its computer systems and sensitive information (including personal information of veterans and their beneficiaries) will remain exposed to an unnecessary and increased risk of unauthorized use, disclosure, tampering, theft, and destruction.

Mr. Chairman, this concludes our statement today. We would be happy to answer any questions you or other Members of the Subcommittee may have.

Contacts and Acknowledgments

If you have any questions concerning this statement, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512–6244, wilshuseng@gao.gov, or Valerie C. Melvin, Director, Information Management and Human Capital Issues, at (202) 512–6304, melvinv@gao.gov. Other individuals who made key contributions include Charles Vrabel and Anjalique Lawrence (assistant directors), Nancy Glover, Mary Marshall, and Jayne Wilson.

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

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General (OIG) work on VA's implementation of the *Federal Information Security Management Act of 2002* (FISMA), which requires that VA develop, document, and implement an agency-wide information security program. Accompanying me is Mr. Michael Bowman, Director, Information Technology and Security Audits. In March 2010, we issued a report, *Fiscal Year 2009—Federal Information Security Management Act Assessment,* that provided 40 recommendations for improving VA's information security program.

Seven years after FISMA's enactment, we continue to report significant deficiencies with controls supporting VA's information security program, which could have potentially alarming consequences. While VA has made progress defining policies and procedures supporting its agency-wide information security program, it faces significant challenges implementing effective access controls, system interconnection controls, configuration management controls, and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction. Because of the significant security deficiencies, the OIG's independent financial statement auditors concluded that VA's implementation of its agency-wide information security program constitutes a material weakness for financial reporting. I will focus on VA's progress and the challenges it faces in implementing key elements of its information security program and system security controls.

BACKGROUND

Sound information security practices are vital to the Federal Government because secure systems and networks are needed to support critical programs and operations. The need for a vigilant approach to information security is apparent as demonstrated by well publicized reports of information security incidents, the wide availability of hacking tools on the internet, and the advances in the effectiveness of attack technology. Without proper safeguards, VA computer systems are vulnerable to intrusions by groups with malicious intent, who can obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. In the past, VA has reported security incidents in which sensitive information has been lost or stolen, including personally identifiable information, exposing millions of Americans to the loss of privacy, identity theft, and other financial crimes.

Concerned by reports of significant weaknesses in Federal computer systems, Congress passed FISMA in 2002, which requires agencies to develop and implement an information security program, evaluate security processes, and provide annual reports. FISMA sets forth a framework for establishing information security controls over systems that support Federal operations and requires annual independent evaluations by the Inspectors General or independent external auditors. To assess compliance with the requirements of FISMA, the Office of Management and Budget (OMB) prepares annual reporting instructions requiring each agency to provide information summarizing their ability to secure their information systems and data. Additionally, OMB requires the Inspectors General to independently evaluate the agency's performance in a number of security areas and provide their results to OMB as part of the annual reporting requirements under FISMA. Historically, OMB's annual reporting instructions have focused on whether agencies have developed appropriate policies, procedures, and practices supporting their information security program. While our work has addressed OMB's reporting requirements, we have also performed comprehensive testing of general and technical information security controls that are designed to protect VA's mission critical systems and data. We believe our audit findings and recommendations provide a solid foundation for improving the effectiveness of VA's information security program and assisting VA in meeting the information security objectives of FISMA.

OIG AUDIT RESULTS

Our annual audit work includes determining the extent VA complies with FISMA's information security requirements, information security standards developed by the National Institute of Standards and Technology, and the annual reporting requirements from OMB. During our work, we assess VA's information security policies and procedures, observe operational controls, and test technical controls over general support systems and major applications.

Information Security

Our fiscal year (FY) 2009 review found VA made progress implementing elements of its agency-wide information security program. In recent years, VA issued VA Directive and Handbook 6500, *Information Security Program,* to define high level policies and procedures supporting its agency-wide information security program. In FY 2009, VA initiated the formal certification and accreditation of approximately one-third of its major systems—a process designed to provide assurance that security controls are adequately protecting critical systems and data. Also, VA conducted privacy impact assessments on many systems with the goal of identifying and reducing unnecessary holdings of personally identifiable information throughout all VA systems. VA has also established a new risk assessment methodology that addresses deficiencies identified by the OIG in prior years. Recently, VA implemented some technological solutions, such as secure remote access, application filtering, and portable storage device encryption to improve the security control protections over its mission critical systems and data.

In addition to our audit work, VA's Certification and Accreditation Program and internal security reviews have identified over 11,000 plans of action and milestones (action plans) that need to be addressed to remediate system security deficiencies. In the near term, VA must complete a large number of these action plans to provide assurance that system security controls adequately protect mission critical systems. Our testing identified a significant number of action plans that were prematurely closed without sufficient documentation or testing to demonstrate that system security weaknesses were fully addressed. Without adequate testing and supporting documentation, VA cannot justify the closure of the action plans or provide assurances that corresponding information security risks were fully mitigated or eliminated.

Access Controls

During system testing, we identified significant weaknesses with access controls designed to protect VA mission critical systems from unauthorized access, alteration, and destruction. For example, we identified a large number of weak passwords on application servers, databases, and networking devices supporting systems at most VA facilities tested. The presence of weak passwords is a well-known security vulnerability that allows malicious users to easily gain unauthorized access to mission critical systems.

We noted that password settings were not configured to enforce strong passwords on some financial management systems and domain controllers. As identification and authentication controls are primary defense mechanisms against password attacks, enforcement of a strong password policy is essential for preventing unauthorized access to these systems. We also identified numerous user accounts with unnecessary system privileges and unauthorized user accounts that were not supported with formal access authorizations. To enforce comprehensive access controls, VA needs to periodically review system user accounts to ensure that system permissions do not exceed the users' functional responsibilities.

Network access controls are important for providing logical security over interconnected systems and data. We noted that most VA medical facilities were not appropriately using network segmentation to restrict access to their sensitive medical devices and network segments. Consequently, we were able to gain unauthorized access to sensitive sub-networks while at VA medical facilities and from remote locations throughout the enterprise. The proper use of network segmentation for restricting access to sensitive medical devices is critical for the security and operational stability at VA's medical centers.

System Interconnections

During testing of system interconnections, we noted that VA had not identified, managed, or monitored a significant number of VA system connections. In many cases, VA had not maintained appropriate interconnection agreements to establish and govern the security requirements for those external network connections. VA is in the process of cataloging all system interconnections, but unknown system interconnections may exist. The lack of comprehensive monitoring of the external network interconnections prevents VA from effectively detecting and responding to network intrusion attempts in accordance with FISMA. Consequently, an attacker could penetrate VA's internal network and systems over an extended period of time without being detected. To improve its ability to monitor and respond to malicious network activity, VA plans to reduce and consolidate all external network connections into four major gateways over the next several years.

Configuration Management

Configuration management controls ensure that only authorized, tested, and protected systems are placed into operation. We identified significant weaknesses with configuration management controls designed to protect VA's mission critical systems and data from unauthorized access, alteration, or destruction. More specifically, our testing revealed unsecure web application servers, critical application servers hosting vulnerable third-party applications and system software, and user permissions that exceed the user's functional responsibilities on critical database platforms.

For example, we identified several instances of VA hosting unsecure web services that could allow a malicious user to exploit certain vulnerabilities and gain unauthorized access to VA systems. Our testing identified several VA Web sites using outdated encryption modules and one Web site accepting sensitive information over unencrypted internet sessions. We also noted several database platforms providing system functions or hosting outdated system software that could allow any system user to gain unauthorized access to mission critical data and potentially alter the operation of the database. To improve performance in this area, VA needs to implement a comprehensive enterprise-wide patch and vulnerability management program that will continuously identify and remediate security vulnerabilities impacting mission critical systems.

Contingency Plans and Testing

Our review of system contingency plans and testing revealed many instances where VA facilities did not validate whether system owners could restore mission critical systems at a remote processing site to ensure continuity of operations. In its annual FISMA report to OMB, VA reported it had successfully tested the viability of 93 percent of its system contingency plans. Based on our sample, VA provided evidence that only 56 percent of its system contingency plans were successfully tested. Our information was derived from evaluating evidence of actual system contingency plan test results while VA compiled information reported from local managers.

During testing, some VA facilities performed "table-top" testing which involved high level discussions of recovery procedures. However, "table-top" testing does not involve deploying equipment and personnel, and should not be considered a substitute for full contingency plan testing. Without in-depth and realistic contingency plan testing, VA cannot provide assurance that mission critical systems can be readily restored in the event of a disaster or a service disruption.

Recommendations and Corrective Actions

Our FY 2009 report provided 27 current recommendations to the Assistant Secretary for Information and Technology for improving VA's information security program. The report also highlighted 13 unresolved recommendations from prior years' assessments for a total of 40 outstanding recommendations. During FY 2009, VA successfully addressed eight outstanding recommendations from our prior FISMA assessments.

Overall, we recommended that VA focus its efforts in the following areas:

- Remediating information security weaknesses that contribute to the material weakness reported in the annual audit of VA's consolidated financial statements.
- Taking an agency-wide approach for addressing action plans as opposed to developing corrective actions based on specific sites and systems.
- Establishing effective processes for identifying and responding to malicious network activity.
- Implementing automated mechanisms for the continuous monitoring and remediation of security weaknesses impacting VA's mission critical systems.

In response to our report, VA concurred with all findings and recommendations. The Assistant Secretary stated that action plans are currently being developed for each recommendation and detailed plans will be provided to the OIG in a separate response. The Assistant Secretary's response also stated that VA continues to make progress improving the effectiveness of its information security program. More specifically, VA's efforts have contributed to significant reductions in the number of outstanding plans of actions and milestones, a more effective risk assessment methodology, and improvements in privacy impact assessments for minor applications that hold sensitive data. The OIG will continue to evaluate VA's progress during the FY 2010 assessment.

Conclusion

Well publicized information security breaches at VA demonstrate that weaknesses in information security policies and practices can expose mission critical systems and data to unauthorized access and disclosure. While VA has made progress defining policies and procedures supporting its agency-wide information security program, its highly decentralized and complex system infrastructure poses significant challenges for implementing effective access controls, system interconnection controls, configuration management controls, and contingency planning practices that will adequately protect mission critical systems from unauthorized access, alteration, or destruction. Until VA fully implements key elements of its information security program and addresses our outstanding audit recommendations, VA's mission critical systems remain at an increased and unnecessary risk of attack or compromise.

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

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

Good morning Chairman Mitchell, Ranking Member Roe, and Members of the Subcommittee. Thank you for your invitation to discuss the current status of information security at the Department of Veterans Affair (VA) as well as VA's compliance with the Federal Information Security Management Act (FISMA) of 2002. With me today are Mr. Jaren Doherty, Acting Deputy Assistant Secretary for Information Protection and Risk Management, Mr. Jan Frye, Deputy Assistant Secretary for Acquisition & Logistics, and Mr. Fred Downs, Chief Procurement and Clinical Logistics Officer for the Veterans Health Administration representing VA. We are focused on moving the Department to a much more secure posture than that which currently exists.

Information Security remains a critical challenge for both federal and private sector enterprises. While our ability to defend our networks and systems has increased, so too, has the sophistication of our attackers and the desire of those who use our systems for faster and broader access to the information and systems we protect.

Four years after the 2006 theft of a Veterans Affairs laptop containing information on millions of veterans, that incident still reverberates throughout the IT organization and the entire VA. Over the last 4 years, thanks to the support of this Committee, we have made significant changes, including the implementation of an Information Protection organization of over 500 people, and of course, the consolidation of all IT assets under the Assistant Secretary. Those changes have been accompanied by a vast improvement in the information protection processes across the entire VA. Our overall improvement on the Department's security posture is accompanied by actual improvements in the security of our information assets. FISMA is focused on making sure we have done the correct thinking about the risks our systems face and the levels of protection each requires, as well as implemented solutions that actually improve security. VA has put in place a plan to employ many of the successful approaches and technologies used by effective, large-scale private sector organizations to ensure that we have visibility into and control over every aspect of our electronic enterprise. This approach is described later in my testimony.

Our own challenges in information protection remain the scope and scale of the missions VA must accomplish. As we protect Veterans' health information from unwanted access, we must balance that with the fact that the same information must be available immediately to the professionals who need it to serve the Veteran. As we seek to control and protect our Veterans' information anywhere it exists within our extended supply chain (including private sector and federal sector partners), we must recognize the fact that the VA cannot perform its critical mission of caring for our Veterans without outside help and services. And while it is our desire to have already implemented a fully robust, comprehensive, audited, foolproof information security posture, our practical reality is that changing the infrastructure, policies, culture, and practices of the 850,000 people who show up every day across this Nation to serve our Veterans is a massive undertaking. Over the last 4 years, we have made quantifiable progress. Over the next year, we will make greater strides. Am I satisfied with where we are? No. Our goal must be to be the best in Federal Government, and comparable with good private sector enterprises, on our information security practices. With your support, we will continue to work very hard at achieving that goal during my tenure as CIO at VA.

Even with all we have accomplished, we still experience security and privacy incidents–the large majority of them from paper-based incidents. Except for a few, these incidents usually involve the sensitive personal information on a small number of individuals. Nonetheless, we consider any data breach to be serious if Veterans' or employees' sensitive personal information is at risk—no matter the number. Many of these incidents are the result of human error and carelessness, which is why it is so important to establish a culture and a strong environment of awareness and individual responsibility. The training and education of our workforce is probably the single most important action. While it is impossible to predict or prevent every security or privacy incident, it is the primary goal of VA's information protection program.

On September 18, 2007, VA completed the publication of VA Handbook 6500. This handbook outlines the standard for the VA Information Security program; and successfully sets the tone for cyber security procedural and operational requirements Department-wide to ensure compliance with FISMA and the Information Security provisions of title 38 of the U.S. Code. It also provides for the security of VA information and information systems.

Today, with the strong support of this committee, a centralized and strengthened information protection program has been established to ensure safeguarding of all VA sensitive data and to fulfill our mission to:

> *"Serve our Veterans, their beneficiaries, employees and all VA stakeholders by ensuring the confidentiality, integrity, and availability of VA sensitive information and information systems."*

Our vision at OIT and within our Office of Information Protection and Risk Management is to provide world class information security and privacy for VA, Veteran information and all information systems operated by VA. We are making great strides towards this vision and achieving our information protection program goals which are to:

- Protect the overall VA information security and privacy posture to ensure confidentiality, integrity, and availability of information
- Integrate risk and performance management into information security and privacy governance processes
- Ensure alignment of VA security and privacy policy and standards with federal guidelines and best practices
- Enable the VA mission through integration of standardized information security and privacy processes
- Promote an environment where every employee's and contractor's action reflect the importance of information security

Office of Information Technology Oversight Compliance (ITOC)

The Office of Information Technology Oversight and Compliance (ITOC) was established in 2007 and made an immediate impact VA-wide. ITOC used innovative assessment tools and created comprehensive checklists to establish review standards in nearly every aspect of IT operations. ITOC is a highly effective organization that provides critical information to the VA Chief Information Officer.

Today, ITOC has 128 full-time employees, who have successfully completed 1332 assessments at VA facilities to include Medical Centers, Community Based Outreach Centers (CBOCs), Vet Centers, and Regional Offices; ITOC is also helping to effect real change to improve VA's FISMA compliance efforts, and continues to work with each VA Administration and staff office to mentor, train, and coach personnel to ensure a proactive organizational environment to protect sensitive information entrusted to us.

ITOC efforts have had a measurable effect on improving VA's FISMA compliance efforts. ITOC performs the continuous monitoring phase of the Certification and Accreditation (NIST 800–37) of VA systems for IT security controls in an ever evolving environment with continual emerging threats against network security controls. In addition, ITOC assessments document known shortcomings or risks to VA's network and IT infrastructure through creation of Plan of Action and Milestones (POA&Ms). These POA&Ms are created in VA's Security Management and Reporting Tool (SMART) database which directly tracks and ensures there is proper resourcing for correction.

Currently, ITOC works in collaboration with the Office of Information Protection Risk Management (IPRM) to conduct VA's Security Control Assessments (SCA). This combined endeavor maximizes our experience as well as technical knowledge to better ensure compliance.

Information Security and Risk Management Office

After the 2006 laptop theft, VA promised to make protecting Veterans' data a priority. In response, VA quickly established IPRM to provide frontline defense of Veteran's sensitive data on a 365 day-a-year, 24/7 basis for one of the Nation's largest Federal Government agencies and the largest health care provider in the country. IPRM's information security staff includes over 700 dedicated staff supporting over 300 VA facilities, almost 300,000 employees, and 333,000 computers. IPRM's vanguard staff includes the Information Security Officers (ISOs), a facility-based staff whose primary role is to ensure end users are protecting sensitive data. Like ISO's, Privacy Officers are facility-based to ensure the use of personally identifiable information (PII) related to Veterans that is collected by VA is limited to the information that is legally authorized and necessary.

IPRM's Network Security Operations Center (VA–NSOC) provides continuous round-the-clock monitoring of VA's network protecting, responding to, and reporting threats. These personnel are responsible for deterring, detecting, and defeating anything that might adversely affect VA networks and systems. On an average day, VA–NSOC monitors over 1.29 billion web requests per week and prevents over 1.7 million viruses a year frominfecting the VA network. VA–NSOC monitors23 million emails received by VA a week. From this total over 16.4 million emails are blocked due to their potential for cyber crime from bad reputation servers or because they are SPAM.

Investments Have Transformed An Agency's Performance

To provide some historical context, in 2006 VA identified several weaknesses which included:

- Limited ability to scan our systems very limited Network Security Operations Center capabilities
- No investigative procedures for malicious software and forensics
- No visibility of routing architecture beyond the core VA Wide Area Network
- Limited Deployment of Network Intrusion Protection Systems (40 nationwide)
- No centralized patch reporting and validation process
- No visibility of the desktops within VA
- No disaster back-up site for the Security Operations Center
- No Change Management or Configuration Control mechanisms

VA's security program has been almost completely re-invented since 2006. Significant investments in centralization and infrastructure, staff, training, and VA-wide end user education have transformed VA's information security and privacy outcomes and FISMA performance. A metrics-based, customer-centric, performance-based approach, has enabled our security program to turn around its performance in 3 years—a remarkable achievement by any standard.

I will highlight some of the outcomes to show what VA has accomplished in the past 3 years:

- VA established a 24x7 monitoring and defense of VA enterprise network core
- There is 100 percent visibility and 24x7 monitoring of anti-virus consoles
- There is 100 percent visibility and 24x7 monitoring of host based intrusion prevention system consoles
- VA established 24x7 monitoring of 160 network intrusion prevention systems deployed Nationwide
- There are two geographically dispersed operations centers with full redundancy and fail over capabilities
- There is monitoring and management of 84 Terabytes of data a week routed over core Infrastructure
- There is monitoring and management of 41 Terabytes of data a week routed through internet gateways
- VA has established a fully mature change control process

Major Initiatives Will Position VA's Information Protection Program

Two key investment programs for OI&T and IPRM in 2010 are achieving visibility to the desktop and complete medical device isolation architecture for VA medical devices. Both OI&T and IPRM have committed all available resources to accomplishing these top two priorities. These priorities are absolutely essential to creating a 21st century, world class security program.

VA Visibility to the Desktop Initiative

Ongoing attacks against VA systems, coupled with pressure to use Web 2.0 technology, compelled VA to augment desktop visibility in order to provide adequate en-

terprise protection, and ultimately, safeguard the personal information of our Nation's Veterans.

Our most important initiative to date is to mandate that the VA–NSOC has visibility into all devices connected to the VA network by September 30, 2010. "Visibility to the Desktop" is defined as the ability to, at any given time, look at the status of all machines in the network from a central location at the enterprise level. This includes the hardware, software, patch level, level of security compliance, and membership of the administrative group. This is a huge security tool for us, and it means that VA can review and run reports on any of the 333,000 machines on our network. This also gives VA the ability to apply patches which will greatly improve the security of the network.

Challenges to achieving this goal over the next 4 months will be trying to get consistent implementation and configuration of VA-approved scanning and management tools across such a large field organization, as well as standardizing facility participation in VA-wide reporting requirements. Again, I want to emphasize the entire OI&T operation is committed to this effort. Without full visibility, we cannot have an effective information security program—we must be able to see what is out there on our networks, identify the problems and risks, and provide the field with resources needed to tackle emerging issues.

We have put together 30, 60 and 90 day plans to fix these inconsistencies while simultaneously leveraging all available resources in order to accomplish this vital task. VA leadership and field personnel met at an offsite retreat in Washington, DC, in March 2010, to determine the vision, priorities, and next steps to achieve this goal. VA has launched Phase 1 of the initiative which involves inventory, antivirus, host-based intrusion prevention system, patch management, and scanning and vulnerability management with the primary goal of protecting the VA network.

Visibility to the Desktop Initiative will be achieved by providing agent-based, multi-dimensional automation with the following critical operational components:

- Installation and implementation of an enterprise tool that provides data scanning in real time for asset discovery, missing patches, remediation, identification of local administrators, operating, hardware and security system status, custom reports and identification of installed applications.
- Installation of an enterprise-wide forensic tool deployed to examine live systems on the network, provide E–Discovery, instantly capture volatile data in memory, remediate compromised systems and be able to search multiple machines for malware.

Protecting VA Medical Devices through Isolation Architecture

VA faces a critical challenge in securing our medical devices from cyber threats—and securing them is among the highest priorities for VA. VA is the largest medical care provider in the Federal Government with over 50,000 networked medical devices. VA defines a medical device as any device that is used in patient health care for diagnoses, treatment, monitoring, or has gone through the Food and Drug Administration's (FDA) premarket review process. (Note: This usage is not necessarily the same as the use of the term 'device' in the Federal Food, Drug, and Cosmetic Act.)"

The major challenge with securing medical devices is that, because their operation must be certified, the application of operating system patches and malware protection updates is tightly restricted. This inherent vulnerability can increase the potential for cyber attacks on the VA trusted network by creating risk to patient safety. When medical devices are not adequately protected, they can and have been compromised at VA. Over 122 medical devices have been compromised by malware over the last 14 months. These infections have the potential to greatly affect the world-class patient care that is expected by our customers. In addition to compromising data and the system, these incidents are also extremely costly to the VA in terms of time and money spent cleansing infected medical devices.

In 2009, VA mandated that all medical devices at VHA facilities connected to the VA network implement a medical device isolation architecture (MDIA) using a virtual local area network (VLAN) structure. To accomplish this, IPRM has initiated a medical device protection program (MDPP). This program ensures there are pre-procurement assessments for medical devices and outlines a comprehensive protection strategy that encompasses communications, training, validation, scanning, remediation, and patching for the medical devices.

OIT and IPRM have committed to securing all VA medical devices through isolation architecture by December 31, 2010. Major baselines for the project have been established, and the VA's more than 50,000 medical devices will all have isolation architecture established by the end of this year.

In addition to the visibility to the desktop initiative and medical device isolation architecture, other VA IPRM security and FISMA priorities for 2010 are:

- Remediating unresolved Plan of Action and Milestones (POA&M) while focusing efforts on addressing high risk system security deficiencies and vulnerabilities
- Implementing control mechanisms to ensure sufficient supporting documentation is captured in the SMART database to justify POA&M closure
- Employing mechanisms to ensure VA password complexity standards are enforced on all systems across the enterprise
- Initiating periodic reviews of user accounts to identify and eliminate incompatible system functions, system permissions in excess of required functional responsibilities, and unauthorized system user accounts
- Implementing VLAN controls to appropriately restrict access to sensitive network subnets at VA medical centers (VAMCs)
- Identifying external network connections and ensuring appropriate Interconnection Security Agreements and Memorandums of Understanding are in place
- Applying automated mechanisms to periodically identify and remediate system security weaknesses on VA's network infrastructure, database platforms, and web application servers across the enterprise
- Executing procedures to ensure VA contracts contain information security compliance clauses consistent with the FISMA
- Implementing remediation plans to address system security weaknesses found during vulnerability assessments of VA systems
- Initiating periodic reviews of security violations and enabling system audit logs on VA financial management systems
- Establishing a system development and change control framework that will integrate information security throughout the lifecycle of each system
- Applying technological solutions to monitor security for all systems and network segments supporting VA programs and operations
- Developing and testing an integrated continuity of operations plan in accordance with VA Directive and Handbook 0320, *Comprehensive Emergency Management Program*
- Implement effective continuous monitoring process that will incorporate consistent test methods, test procedures, and other testing elements to more accurately measure security control effectiveness
- Creating mechanisms for updating key elements in system security plans to include inventory of systems such as hardware, software, database platforms, and system interconnections
- Developing a comprehensive system inventory listing and expanding data calls for identifying minor applications to include all VA lines of business

Conclusion

In closing, protecting Veteran information is crucial to VA's mission. A breach in security can hinder our ability to perform critical operations, put Veterans at risk, and ultimately result in a loss of public trust. VA is making significant progress in creating a solid environment of vigilance and awareness regarding individual responsibility in the area of information protection—the centerpiece of our overall program.

Moving forward, VA will continue to combat security threats through critical initiatives including Security Improvement Program, visibility to the desktop, medical device protection program, and our ongoing efforts to educate our VA end users. We will continue to take proactive steps to meet the daunting challenges of new technology, such as evolving social media, cloud computing, mobile media, and advanced interconnectivity. We will meet our milestones as outlined in this testimony, to build one of the top security programs in the Federal Government.

I remain personally committed to continually working toward establishing a world class security environment wherein we can fully safeguard the sensitive and private information of our Veterans and employees-and all sensitive information entrusted to us.

MATERIAL SUBMITTED FOR THE RECORD

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 20, 2010

Honorable Gene L. Dodaro
Comptroller General
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Comptroller General Dodaro:

Thank you for the testimony of Gregory C. Wilshusen, Director of Information Security Issues, accompanied by Valerie C. Melvin, Director of Information Management and Human Capital Issues at the U.S. House of Representatives Committee on Veterans' Affairs Subcommittee on Oversight and Investigations hearing that took place on May 19, 2010, entitled "Assessing Information Security at the U.S. Department of Veterans Affairs."

Please provide answers to the following questions by Friday, July 2, 2010, to Todd Chambers, Legislative Assistant to the Subcommittee on Oversight and Investigations.

1. In May 2006, VA suffered a debilitating security breach in which the personally identifiable information of over 26 million veterans and active duty personnel stored on a hard drive was stolen from the home of a VA employee. Is veterans' information more secure now that it was then?
2. You mentioned in your statement that VA is reporting an increasing number of security incidents. Why is that?
    a. Does that mean VA's security controls are ineffective?
3. How does VA's information security program compare to other Federal agencies?
4. What are the top three things that VA should focus on now to strengthen security over its systems and information?
5. VA is implementing its new IT project management guidance—the Project Management Accountability System (PMAS). What is the status of VA's PMAS implementation?
    a. Does this guidance include any provisions for information security?

Thank you again for taking the time to answer these questions. The Committee looks forward to receiving your answers. If you have any questions concerning these questions, please contact Martin Herbert, Majority Staff Director for the Subcommittee on Oversight and Investigations at (202) 225–3569.

Sincerely,

Harry E. Mitchell
Chairman

MH:tc

U.S. Government Accountability Office
Washington, DC.
July 2, 2010

The Honorable Harry E. Mitchell
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
U.S. House of Representatives

Dear Chairman Mitchell:

This letter responds to your request dated May 20, 2010, to provide answers to five questions related to the May 19, 2010, hearing on assessing information security at the Department of Veterans Affairs (VA). Your questions and our responses follow.

Question 1: *In May 2006, VA suffered a debilitating security breach in which the personally identifiable information of over 26 million veterans and active duty personnel stored on a hard drive was stolen from the home of a VA employee. Is veterans' information more secure now than it was then?*

In some respects veterans' information is more secure now than it was in May 2006, but it is still vulnerable to unauthorized disclosure and modification. In the 4 years since the 2006 security breach, VA has taken several steps to strengthen information security. In October 2006, the department moved to a centralized management model as part of organizational changes implemented to improve service to veterans. In September 2007, we reported that VA was addressing the problem of unencrypted laptops, and that 244 of 248 laptops we examined at eight locations had been encrypted.[1] VA also finalized guidance for developing, documenting, and implementing the elements of the information security program, and filled the position of chief information security officer. Additionally, VA has taken steps to clearly define responsibilities of key information security officials and to improve coordination among them. Another action that VA is currently undertaking is implementing the Federal Desktop Core Configuration initiative, which should help the department to better safeguard its workstations that use the Windows XP and Vista operating systems and protect sensitive information.

However, much work remains to appropriately secure veterans' information. As recently reported by the VA Inspector General and VA's independent auditor, significant control weaknesses continue to exist in each of five major categories of security controls: (1) access controls, which are intended to ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations, which is intended to prevent significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which is to provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. For example, VA had deficiencies in the controls intended to prevent, limit, and detect unauthorized access to its computer systems and information. As a result, veterans' personal information remains at unnecessary risk of unauthorized disclosure and inadvertent or deliberate misuse.

Question 2: *You mentioned in your statement that VA is reporting an increasing number of security incidents. Why is that?*

a. Does that mean VA's security controls are ineffective?

There are likely two reasons why VA has been reporting an increasing number of security incidents over the past 3 years. The first reason relates to improvements in VA's incident management capability. Since the May 2006 data theft, VA has realigned and consolidated two centers with responsibilities for incident management, as well as developed and documented key policies and procedures. For example, it has developed an incident report template to assist VA personnel in reporting incidents to the consolidated center within 1 hour of discovering an incident. In addition, VA employees were required to take security and privacy training, which may have heightened their awareness of their responsibility to report incidents involving loss of personal information. These actions are, perhaps, contributing factors to VA having reported the highest number of incidents in comparison to 23 other major Federal agencies during fiscal years 2007 through 2009.

The second reason is the likelihood that the number of attacks or incidents is increasing, although we cannot be certain of this because the number of *undetected* attacks or incidents is not known. We have previously reported that the threats to Federal systems and critical infrastructure are evolving and growing. The fact that VA has been reporting an increasing number of security incidents over each of the past 3 years is consistent with the experience of other Federal agencies. To illustrate, the government-wide number of security incidents reported by Federal agencies to U.S. CERT has increased dramatically from about 5,500 in fiscal year 2006 to about 30,000 in fiscal year 2009, an increase of over 400 percent. Across the government, agencies including VA have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

The fact that VA is reporting an increasing number of security incidents does not necessarily mean, in and of itself, that VA's security controls are ineffective because

---

[1] GAO, *Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs,* GAO–07–1019 (Washington, D.C.: Sep. 7, 2007).

even strong controls may not block all intrusions and misuse. However, it does indicate that vulnerabilities remain in security controls designed to adequately safeguard information. Moreover, despite the steps VA has taken to strengthen its information security, both the Office of Inspector General and an independent auditor reported that VA's security controls were ineffective. In VA's fiscal year 2009 performance report, the independent auditor cited failures to remediate known security control deficiencies, enforce policies for passwords, approve changes to systems, and test contingency plans, among other weaknesses.[2] The auditor concluded that IT security and control weaknesses remain pervasive at VA.

Question 3: *How does VA's information security program compare to other Federal agencies?*

Similar to VA, most major Federal agencies have deficient information security programs. As depicted in table 1, our analysis of inspector general, agency, and GAO reports shows that most major agencies had weaknesses in most of the key security control categories for fiscal year 2009.

Table 1: 24 Major Federal Agencies' Control Weaknesses for Fiscal Year 2009

Security control category	Number of major agencies reporting weaknesses	Was VA one of the agencies reporting weaknesses?
Access controls	22	yes
Configuration management	23	yes
Segregation of duties	17	yes
Contingency planning	22	yes
Security management	23	yes

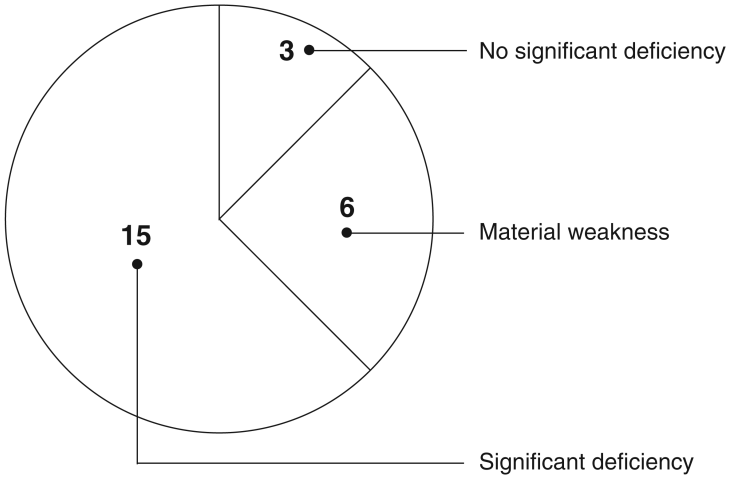
Source: GAO analysis of IG, agency, and GAO reports.

VA was one of six major agencies to report a material weakness in information security over its financial systems and information—the most severe kind of weakness for financial reporting purposes.[3] As illustrated in figure 1, 21 of the 24 major agencies either had a material weakness or significant deficiency in information security over their financial systems.

[2] Department of Veterans Affairs, *FY 2009 Performance and Accountability Report,* (Washington, D.C.: Nov. 16, 2009).

[3] A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

Figure 1: Significant Deficiencies in Information Security Included in 24 Major Agencies' Financial Reporting



Source: GAO analysis of agency performance and accountability report, annual financial report, or other financial statement reports for FY 2009.

VA was also one of the 20 major agencies for which information security was cited as a major management challenge in fiscal year 2009. In part for these reasons, GAO has continued to designate information security as a governmentwide high-risk area since 1997.

Question 4: *What are the top three things that VA should focus on now to strengthen security over its systems and information?*

To address long-standing weaknesses and strengthen VA's information security program, the following three actions are key:

- *Mitigate known vulnerabilities, focusing on high-risk deficiencies and weaknesses.* Over the past several years, GAO, VA's Office of Inspector General, and VA's internal assessments have identified thousands of security deficiencies and vulnerabilities in the department's information systems and practices. Following the May 2006 security incident, VA officials began working on an action plan to strengthen information security controls at the department. In fiscal year 2009, VA's independent auditor reported that while the department continued to make steady progress, many information technology security control deficiencies were not analyzed and remediated across the agency, deficiencies were sometimes closed as corrected in the absence of sufficient and documented support for the closures, and a large backlog of deficiencies remained in the VA plan of action and milestone system. Effective mitigation of these deficiencies could help VA to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data. If these deficiencies are not successfully corrected in a timely manner, VA will continue to lack effective security controls to safeguard its assets and sensitive information.
- *Implement automated mechanisms to monitor systems and networks, and identify and remediate system security weaknesses.* Another action that VA can take to improve securing and monitoring of its systems and networks is to expand its use of automated tools for performing certain security-related functions. Because VA is large and geographically dispersed, increasing automation of key security processes can assist in the efficient and effective implementation of key controls across the entire enterprise. For example, VA can use centrally administered automated diagnostic and analytical tools to continuously monitor network traffic, scan devices across the enterprise to identify vulnerabilities or anomalies from typical usage, and monitor compliance with departmental configuration requirements. In addition, improving the use of automated tools for patch management can increase efficiency in mitigating known vulnerabilities on many systems within the department. In its fiscal year 2009 performance re-

port, VA acknowledged the need to implement monitoring mechanisms and address system security weaknesses. The department plans to have 100 percent of its operational systems in continuous monitoring by the end of fiscal year 2010.

- *Establish and implement oversight and accountability mechanisms to ensure that* management *remains committed and effective in its efforts to implement a comprehensive information security program.* Security programs should have owners at the management level who are held accountable through performance appraisals that can be affected by the results of these measures. In September 2006, VA issued a memorandum that required all senior executive performance plans to include information security as an evaluation element by November 30, 2006. In a September 2007 report, we stated that VA was unable to provide documentation on the performance plan reviews or a documented process for regular review of these plans.[4] Without a process for reviewing senior executives' performance plans on a regular basis to ensure that information security is included as an evaluation element, VA may not have effective management accountability for information security. Accordingly, we recommended that VA develop, document, and implement a process for reviewing on a regular basis the performance plans of senior executives to ensure that information security is included as an evaluation element. The department has stated that it now has in place a process for reviewing these senior executives' performance plans. We plan to verify VA's actions later this year.

Question 5: *VA is implementing its new IT project management guidance—the Project Management Accountability System (PMAS). What is the status of VA's PMAS implementation?*

a. Does this guidance include any provisions for information security?

As of March 2010, VA had begun applying the PMAS management approach to all of the department's IT projects that were planned to deliver new system functionality or enhance existing systems. Initiated in June 2009 by VA's Assistant Secretary for Information and Technology (who serves as the department's Chief Information Officer), PMAS is intended to improve the department's management and oversight of IT projects by requiring that new system functionality be delivered to customers in 6-month increments and that projects be stopped and re-evaluated after missing three consecutive customer delivery milestones. When PMAS was initiated, the Assistant Secretary called a stop to 45 of the department's IT projects that were identified as behind schedule or over budget.

VA has included high-level discussion of information security in its PMAS guidance. Specifically, the department's original (June 2009) PMAS instructions described actions necessary for projects to restart, including development of a system security plan and requirements for how system security will be managed. Subsequent guidance, issued in March 2010, required the development of a project management plan that, according to the department, is to include system security plans and requirements.

Our responses to these questions are based on work that we performed in accordance with generally accepted government auditing standards.

Gregory C. Wilshusen
Director, Information Security Issues

Valerie C. Melvin
Director, Information Management and Human Capital Issues

[4] GAO–07–1019.

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 20, 2010

Honorable George J. Opfer
Inspector General
U.S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Inspector General Opfer:

Thank you for the testimony of Belinda J. Finn, Assistant Inspector General for Audits and Evaluations, Office of Inspector General, U.S. Department of Veterans Affairs, accompanied by Michael Bowman, Director of Information Technology and Security Audits, Office of Inspector General at the U.S. House of Representatives Committee on Veterans' Affairs Subcommittee on Oversight and Investigations hearing that took place on May 19, 2010, entitled "Assessing Information Security at the U.S. Department of Veterans Affairs."

Please provide answers to the following questions by Friday, July 2, 2010, to Todd Chambers, Legislative Assistant to the Subcommittee on Oversight and Investigation.

1. What are the VA's most significant risks related to adequately protecting its systems and sensitive data?
2. What are VA's most significant risks regarding its many system interconnections with external organizations?
3. How is the OIG leveraging the work of the independent financial statement auditors to expand the depth of its FISMA assessments?
4. Moving forward, what steps can VA take to prevent the loss of sensitive data?
5. How has VA's realignment of its Information Technology program in 2006 impacted the implementation of the Department's security program?
6. What are some of the criticisms regarding FISMA law and how has it impacted OIG's evaluation of VA's information security program?
7. What is the role of FISMA's Certification and Accreditation process for securing Federal information systems?
8. What are VA's most significant risks related to adequately protecting its systems and sensitive data?

Thank you again for taking the time to answer these questions. The Committee looks forward to receiving your answers. If you have any questions concerning these questions, please contact Martin Herbert, Majority Staff Director for the Subcommittee on Oversight and Investigations at (202) 225–3569.

Sincerely,

Harry E. Mitchell
Chairman

MH:tc

U.S. Department of Veterans Affairs
Office of Inspector General
Washington, DC.
June 21, 2010

The Honorable Harry E. Mitchell
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

This is in response to your May 20, 2010, letter following the May 19, 2010, hearing on *Assessing Information Security at the U.S. Department of Veterans Affairs.* Enclosed are our responses to the additional hearing questions.

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

Sincerely,

/s/ Richard J. Griffin for
GEORGE J. OPFER

Enclosure

Questions from the Honorable Harry Mitchell For Belinda Finn, Assistant Inspector General for Audits and Evaluations Office of Inspector General, U.S. Department of Veterans Affairs, Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, United States House of Representatives, Hearing on *Assessing Information Security at the U.S. Department of Veterans Affairs*

Question 1: What are VA's most significant risks related to adequately protecting its systems and sensitive data?

Response: Assessments conducted under the Federal Information Security Management Act (FISMA) identified three areas of concern:

- Unauthorized Access—Default passwords, weak passwords, and vulnerable third party applications provide well-known attack points for malicious users to gain unauthorized access to mission critical systems.
- Contractor Security—VA faces significant challenges providing effective oversight to ensure contractors are meeting VA's information security requirements. Our review of a specific service provider managing multiple active contracts also revealed that VA has not implemented effective procedures to mitigate the risks of unauthorized access and disclosure of sensitive veteran information. VA will remain at risk unless it can ensure that all staff and contractors comply with relevant information security policies and procedures.
- External Organizations—VA's system interconnections with external organizations, such as affiliates, also pose significant risks to VA systems and data.

Question 2: What are VA's most significant risks regarding its many system interconnections with external organizations?

Response: The most significant risks regarding its many system interconnections with external organizations are:

- Unencrypted Protocols—Many of these system interconnections utilize unencrypted protocols to transfer sensitive veteran data. Consequently, interconnection data is vulnerable to interception by attackers outside the network.
- Monitoring—VA does not monitor most of its system interconnections with external organizations, providing ample opportunities for attackers to penetrate VA's network without being detected.
- Controls—While VA has established interconnection agreements with most external organizations hosting VA sensitive data, it has not implemented controls to ensure that external organizations are adequately protecting sensitive veteran data in accordance with VA policies and procedures (End Point Security).

Question 3: How is the OIG leveraging the work of the independent financial statement auditors to expand the depth of its FISMA assessments?

Response: We expanded the scope of the consolidated financial statement audit to include testing of security controls, which directly relates to our FISMA assessment as well as the independent audit of VA's financial statements.

In connection with the evaluation of VA's Consolidated Financial Statements, our independent auditors perform information security testing at VA's three major data centers and include assessments of mission critical financial management systems, data bases, web applications, network devices, and general support systems. The results of this work directly support the OIG's evaluation of VA's information security program in accordance with FISMA.

The expanded scope has enabled us to increase the number of FISMA site visits from 12 facilities in FY 2009 to 20 facilities in FY 2010. This expanded coverage enables us to identify trends and systemic issues, draw better conclusions, and make recommendations regarding the effectiveness of VA's information security program.

Question 4: Moving forward, what steps can VA take to prevent the loss of sensitive data?

Response: VA needs to implement safeguards to ensure that external organizations are adequately protecting sensitive veteran data in accordance with VA policy and FISMA. VA should ensure that all service provider contracts include provisions to implement information security protections in accordance with VA policy and procedures. VA also needs to establish a complete inventory of all hardware that hosts VA sensitive data and ensure that storage devices are authorized and fully encrypted.

Further, VA must implement procedures to sanitize all storage devices that are no longer used to host sensitive data. VA also needs to fully deploy software that will prevent personnel from transferring VA sensitive data to unencrypted and unauthorized personal storage devices.

Question 5: How has VA's realignment of its Information Technology (IT) program in 2006 impacted the implementation of the Department's information security program?

Response: The centralization of IT functions has allowed VA to develop agency-wide policies and procedures supporting VA's information security program. However, our annual FISMA evaluations continue to show that VA has not implemented effective controls to enforce VA's information security policies and procedures.

The centralization has facilitated the development and implementation of the Certification and Accreditation program and the Privacy Impact Assessments program across the agency. However, our FISMA assessments have concluded that VA's Certification and Accreditation and Privacy Impact Assessment programs do not adequately identify and mitigate significant information system security risks. For example, the Certification and Accreditation program did not identify significant access control weaknesses that were discovered during the OIG's annual FISMA assessment. Privacy Impact Assessments did not consider whether VA sensitive information was stored on minor applications hosted at VA medical facilities and other program offices.

Moreover, VA still has a high number of decentralized legacy information systems and networks and continues to struggle with implementing consistent and effective information security controls across all systems and networks.

Question 6: What are some of the criticisms regarding the FISMA law, and how has it impacted OIG's evaluation of VA's information security program?

Response: Since its passage, some believe that FISMA is a paperwork intensive exercise that has identified vulnerabilities but has not significantly improved information system security controls at Federal agencies.

The OMB Chief Information Officer has also stated that elements of FISMA reporting are based on metrics that focus on compliance reporting rather than information security outcomes. To improve the quality of FISMA reporting in 2010, OMB will require agencies to provide broader information related to their system inventories, critical applications, external connections, identity management, and access controls. The expanded FISMA reporting will assist OMB in determining whether agencies are effectively monitoring information supporting their agency-wide information security programs. For example, collecting data on the number of systems tested for security vulnerabilities will allow OMB to assess the effectiveness of the agency-wide information security program.

Our audit work addresses OMB's compliance reporting requirements under FISMA. More importantly, our work involves substantial testing of general and technical information security controls designed to protect VA's mission critical systems from unauthorized access, alteration, and destruction. Testing of general and technical information security controls helps us offer recommendations that can improve the security posture of VA in areas where significant security risks persist. Our audit findings and recommendations provide a solid foundation for improving the effectiveness of VA's information security program and for assisting VA in meeting the fundamental security objectives of FISMA.

Question 7: What is the role of FISMA's Certification and Accreditation process for securing Federal information systems?

Response: Under FISMA, Certification and Accreditation is a formal process of identifying agency systems and their boundaries, conducting risk assessments of potential security threats and vulnerabilities, establishing minimum sets of security controls to protect agency systems, and performing tests of controls to provide assur-

ance that relative system security risks are addressed or fully mitigated by compensating controls.

Documentation provided in Certification and Accreditation packages include system risk assessments; system security, remediation and contingency plans; and the results of independent security controls analyses.

The Certification and Accreditation process is designed to provide authorizing officials with essential information so they can make credible risk-based decisions on whether to authorize the operation of an information system.

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Washington, DC.
May 20, 2010

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

Dear Secretary Shinseki:

Thank you for the testimony of the Honorable Roger W. Baker, Assistant Secretary for Information and Technology, U.S. Department of Veterans Affairs, accompanied by Jaren Doherty, Acting Deputy Assistant Secretary for Information Protection and Risk Management, Office of Information and Technology; Jan R. Frye, Deputy Assistant Secretary for Acquisition and Logistics, Office of Acquisition, Logistics, and Construction; and Frederick Downs, Jr., Chief Procurement and Clinical Logistics Officer, Veterans Health Administration at the U.S. House of Representatives Committee on Veterans' Affairs Subcommittee on Oversight and Investigations hearing that took place on May 19, 2010, entitled "Assessing Information Security at the U.S. Department of Veterans Affairs."

Please provide answers to the following questions by Friday, July 2, 2010, to Todd Chambers, Legislative Assistant to the Subcommittee on Oversight and Investigations.

1. In a December 30, 2009 letter to Peter Orszag, Director of the Office of Management and Budget, Secretary Shinseki stated that though VA's CIO section report states that contingency plans for 94 percent of VA's systems have been tested in accordance with department policy, the IG indicates that only 50 percent of the contingency plans have been tested. Furthermore, the IG reports that VA's SMART database does not maintain evidence that contingency plan testing was performed for all 581 systems reported to OMB. What do you attribute the differences between your numbers and the IG's?
    a. Also, are there financial and operational considerations that contribute to these differences? If so, please explain in detail the financial and operational aspects.
2. Please explain the FISMA implications in the VA's two recent data breaches.
3. In FY 2009, the VA closed just over 9,000 plans of actions and milestones. There are still approximately 8,615 unresolved plans of actions and milestones, almost half (4,218) of which were overdue. Please explain the reasons for these deficiencies.
4. How does VA enforce the FISMA requirements on contractors and how often?
5. What material weaknesses in the system did the two breaches reported in April uncover?
6. Prior to the April breaches, particularly with the logbook loss, who at the Department of Veterans Affairs was in charge of securing veteran information not maintained in an IT environment? How has this changed since the loss of the logbook?
7. Who is currently responsible for contracts procured by the Medical Centers if they contain programs that may provide the contractor access to veterans' personal information?
8. How will the Department ensure that the information security clause is in every contract whereby veteran information is exchanged between VA and a contractor?

9. How has the General Counsel's office addressed the 500 plus contractors who have refused to sign the contract modifications adding the information security clause?
10. Given the concern that there should not be a reduction in services to our veterans, please respond to the following questions:
    a. Please provide the Committee with a list of the 579 contractors who refused to sign the information security clause.
    b. How many of these contracts are currently providing critical veterans' services?
    c. What will happen to the contracts if the vendor continues to refuse to sign the information security clause?
    d. Will services to our veterans be undermined if VA actively pursues these contractors or discontinues business with them?
11. Both the VA OIG and the GAO had identified areas of weakness at the VA relating to information security, particularly in the areas of access controls, configuration management, segregation of duties, contingency planning, and security management. What steps are being taken by the Department to address these deficiencies? Please provide the Committee with a timeline for full implementation of these measures?

Thank you again for taking the time to answer these questions. The Committee looks forward to receiving your answers. If you have any questions concerning these questions, please contact Martin Herbert, Majority Staff Director for the Subcommittee on Oversight and Investigations at (202) 225–3569 or Arthur Wu, Minority Staff Director for the Subcommittee on Oversight and investigations at (202) 225–3527.

Sincerely,

Harry E. Mitchell
Chairman

David P. Roe
Ranking Republican Member

MH/:tc

Questions for the Record
The Honorable Harry E. Mitchell, Chairman
The Honorable David P. Roe, Ranking Republican Member
Subcommittee on Oversight and Investigations
House Committee on Veterans' Affairs
Assessing Information Security at the U.S. Department of Veterans' Affairs

May 19, 2010

Question 1: In a December 30, 2009 letter to Peter Orszag, director of the Office of Management and Budget, Secretary Shinseki stated that though VA's CIO section report states that contingency plans for 94 percent of VA's systems have been tested in accordance with department policy, the IG indicates that only 50 percent of the contingency plans have been tested. Furthermore, the IG reports that VA's SMART database does not maintain evidence that contingency plan testing was performed for all 581 systems reported to OMB. What do you attribute the differences between your number and the IG's?

Question 1(a): Also, are there financial and operation considerations that contribute to these differences? If so, please explain in detail the financial and operational aspects.

Response: The Department believes that the differences noted are primarily due to the inability of the sites to upload contingency testing documents to the SMART database for review by the OIG. Also, some sites cannot test contingency plans at alternate sites in accordance with existing Department policy due to financial and operational considerations, such as the inability to take mission-critical systems out of production for even a brief period of time. To address these differences, the Department will ensure that all evidence of contingency plan testing is uploaded into the SMART database and will look into revising existing policy requiring alternative site testing of contingency plans.

Question 2: Please explain the FISMA implications in the VA's two recent data breaches.

Response: Federal Information Security Management Act (FISMA) guidance for the protection of Personally Identifiable Information (PII) is defined in the NIST Special Publication (SP) 800–122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). VA already has adequate policies and procedures in place to identify these two incidents as major deficiencies.

In the case of the lost laptop by the contractor, specific processes by OI&T personnel and those within the Office of Acquisitions, Logistics and Construction are currently being put into place to remediate any commercial contracts being awarded without the specific requirements for safe keeping of sensitive and PII information. VA is also analyzing auditing vendors in their security practices to ensure they are complying with these requirements.

Security language in contracts has been a requirement since the first security policy was created in July 1988 (VA Circular 10–88–78). Additionally, VA CIO Memorandum, *Contract Security/Privacy Requirements,* dated August 27, 2008, and VA Secretary Memorandum, *Protecting Information Security and Privacy,* dated February 27, 2009, further established the requirement. VA Handbook 6500.6, *Contract Security,* published March 12, 2010, incorporates content from both memorandums and makes security language in contracts VA policy.

In the case of the lost hard copy binder, although there are policies in place to ensure this type of incident should never have occurred, these policies were not sufficient. VA is in the process of crafting an acceptable security practice that provides more security without hindering medical care.

Question 3: In FY 2009, VA closed just over 9,000 plans of actions and milestones. There are still approximately 8,615 unresolved plans of actions and milestones, almost half (4,218) of which were overdue. Please explain the reasons for these deficiencies.

Response: VA conducts security reviews on information systems which result in Plans of Action and Milestones (POA&M), or deficiencies. A regular review schedule and a continuous monitoring effort produce new deficiencies as new exploits and vulnerabilities are found. This increases the number of deficiencies that VA carried from FY 2009.

However, VA has taken an aggressive approach to removing these deficiencies. Our efforts with projects such as implementation of Federal Desktop Core Configuration (FDCC), visibility to the desktop initiative and increased focus on vulnerability scanning, will systematically remove deficiencies and prevent slippage in remediation schedules to reduce actions becoming overdue.

VA is also implementing a continuous monitoring program with increased oversight capabilities to monitor POA&Ms at each facility and on each information system. This effort prevents occurrences where tasks are not being completed timely and effectively.

To clean up the backlog of overdue POA&Ms, VA created POA&M work groups on November 12, 2008, consisting of representatives from various organizations, including IT Field Operations and Development (FOD), CIOs, Field Security Service (FSS) Information Security Officers (ISOs), Engineering, Development, and the Office of Cyber Security (OCS). This group, co-chaired by the FSS Regional Information Security Directors (RISDs) and IT FOD Certification and Accreditation (C&A) Coordinators, identified and divided POA&Ms into four work groups based on major groupings of systems in the Department FISMA inventory. Each workgroup made recommendations to address POA&Ms based on the following: national waiver requests, identified invalid POA&Ms, and recommended remediation at the National-, Regional-, or Local-level. Currently, the following actions have been taken:

- National waiver requests have been completed
- National-level POA&M points of contact have been appointed by OED, EIE, and the Region 5 IT Director to assist local sites with remediation
- Local sites have been informed of what POA&Ms they are required to complete

IT FOD is chartering a new POA&M initiative in FY10–FY 2011 called the "FISMA Challenge" to further define roles and responsibilities, and take a risk based decision approach to address POA&Ms.

Question 4: How does VA enforce the FISMA requirement on contractors and how often?

Response: VA released a new policy in March 2010, VA Handbook 6500.6, *Contract Security,* which provides a process to ensure that the security clause and appropriate security language are included in VA contracts in which VA sensitive information is stored, generated, transmitted or exchanged, regardless of format and whether it resides on VA or non-VA systems. This process involves a team that includes the Information Security Officer (ISO), the Privacy Officer (PO), the Contracting Officer's Technical Representative (COTR) and the Contracting Officer (CO) in the review of contracts to ensure that the appropriate language for that particular contract is included in the contract. This process applies to the creation of new contracts. The Handbook includes a checklist that helps the team determine the areas within the proposed contract that would have security implications. The Handbook also provides an Appendix that contains 12 pages of reviewed/approved security/privacy language that will be added to contracts, as appropriate. The Handbook also includes the requirement for oversight of contracts. To help provide oversight, Certification and Accreditation (C&A) of applicable contractor systems as well as a new Contractor Security Control Assessment (CSCA) is introduced that can be utilized for monitoring service contracts such as transcription contracts and tele-radiology contracts. A "Contractor Rules of Behavior" is also introduced that outlines a contractor's individual security responsibilities.

Contractors and contractor-provided services are reviewed at least annually for compliance with FISMA requirements. All contractors are required to take security awareness training and sign the "rules of behavior" annually, and VA information security officers validate service provider conformance with FISMA requirements at least annually through reviews of system documentation to ensure security controls are documented and tested, site visits to ensure security controls are in place and operating as stated in the documentation, and interviews with contractors operating these systems.

Question 5: What material weaknesses in the system did the two breaches reported in April uncover?

Response: With the Heritage Health Solutions laptop loss, contractor data security has become a focused issue. Some contracts were found to not have the proper security language in them. The other concern is that some vendors have contracts with the correct security language in place, but are not following the security measures required. VA did not have a way of monitoring the security effectiveness of the many contracts in place.

With the Dallas VAMC's missing binder and clipboard, paper loss has become a more focused issue. All logbooks used in clinical settings, containing either PII or PHI are major vulnerabilities.

Question 6: Prior to the April breaches, particularly with the logbook loss, who at the Department of Veterans Affairs was in charge of securing Veterans information not maintained in an IT environment? How has this changed since the loss of the logbook?

Response: Each service or department seeing patients has procedures in place as dictated by the Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Office to secure all paper copies of information generated, produced or otherwise prepared in the course of business. In response to this breach, the facility has taken steps to identify all log books being used at the Medical Center and begun identifying other means to track patients. The Privacy Office and OI&T have the ultimate responsibility of securing information regardless of the storage environment.

Question 7: Who is currently responsible for contracts procured by the Medical Centers if they contain programs that may provide the contractor access to Veterans' personal information?

Response: VHA revised response: The local Contracting Officer (CO) is responsible for contracts procured by the medical centers if they contain programs that may provide the contractor access to Veterans' information. The CO, Information Security Officer (ISO), and the Privacy Officer (PO) meet during the acquisition planning stage to review the contract requirements and plan how to best protect personal information. Also, the Contracting Officer's Technical Representative (COTR) maintains oversight of the contract during the administration of the contract to insure compliance with the contract terms and conditions as related to the security of IT information. It is a concerted effort of several VA offices, critical personnel and subject matter experts who must address the security of Veterans' personal data.

Question 8: How will the Department ensure that the information security clause is in every contract whereby Veteran information is exchanged between VA and a contractor?

Response: With the implementation of VA Handbook 6500.6, *Contract Security,* a process has been created to ensure that the security clause and appropriate security/privacy language is included in contracts in which VA sensitive information is stored, generated, transmitted or exchanged, regardless of format and whether it resides on VA or non-VA systems.

Effective immediately, the Office of Information and Technology Oversight and Compliance (ITOC), an organization of 128 highly skilled security analysts during each of their upcoming facility assessments, will review the 10 largest dollar amount contracts, 20 randomly selected contracts, and 3 vendors for all contracts that receive or store information on VA clients at that facility to ensure their compliance with VA policy. Any facility with contracts that do not comply with the required security language will be reported to the appropriate VA senior leadership for remediation. Also, the Risk Management Team recently incorporated inclusion of the information security clause into its A–123 Audit Reviews.

Question 9: How has the General Counsel's office addressed the 500 plus contractors who have refused to sign the contract modifications adding the information security clause?

Response: The Office of the General Counsel (OGC) has been providing ongoing, adhoc, informal advice to contracting officers and other procurement staff across the country since Secretary Shinseki's February 27, 2009 Memorandum ordered all VA contracts and other agreements to be examined and analyzed to determine whether the VAAR Security Clauses should be incorporated and modified into existing contracts and agreements and written into future procurement documents. OGC has also participated in various teams working on VHA Memoranda and VA Handbook 6500 groups. OGC's Professional Group V has also provided written guidance to VA procurement attorneys across the country. OGC has further given advice to strategic response teams to help them understand the analyses necessary to resolve the situations involving contractors who refuse to sign modifications adding the VAAR Security Clauses into their contracts.

Analysis

A VHA review had identified 580 contracts in which contractors had not agreed to incorporate the VAAR clauses into existing, open contracts. Further review and analyses with the combined efforts of Information Security Officers (ISOs), Privacy Officers (POs), and Contracting Officers (COs) with OGC guidance produced the following result: only 3 contracts (as of June 25, 2010) still required a resolution of their VAAR security clause status as not all VA or VHA contracts required such modifications or amendments.

For all VA Veterans Integrated Service Networks (VISNs) combined, the data reveals how the 580 contracts/agreements identified were reduced to 60 as of June 11, 2010:

Clause Added	Contract Expired	Contract Terminated	ISO/PO Exemption [1]	Nursing Home Exemption	Contracts/ Agreements At Issue	Grand Total
92	*176*	*6*	*36*	*215*	***60***	***580***

[1] ISO/PO Exemption(s): When ISO/PO analysis suggested the security clauses were not necessary, the requirement was waived and the contract exempted from including the clauses.

Where the contracts were allowed to expire or were terminated, those dropped from the total of scrutinized contracts. ISOs, POs, and COs examined the agreements and found 36 that either did not need or warrant the clauses or were worthy of an exemption from the clause requirements, still maintaining data security and integrity. Finally, non-VA nursing homes/facilities were generating their own Sensitive Personal Information (SPI), Personally Identifiable Information (PII) and/or Personal Health Information (PHI) so that the VAAR clauses, intended to deter the unauthorized use, exposure, or disclosure of VA SPI would not likely be applicable. OGC provided guidance, as requested, to help this analysis. As of June 25, 2010, OGC helped VHA staff reduce the "orphan" cases where the VAAR Security Clause issue had not been resolved to 3 through reaching out to VHA staff, COs, and ISOs in the field.

Contract Expired	Currently With ISO for Review	VAAR Clauses Added	Duplicate K	ISO/PO Exemption	ISO Denied Exemption, Elevated to OGC	Grand Total	Contracts awaiting resolution
5	45	2	1	2	2	57	3 of 22,000

One "duplicate" contract file was found and deleted from the data. Five more contracts had expired, 2 more had the VAAR Security Clauses incorporated by amendment, 45 were undergoing ISO review, 2 more received ISO/PO exemptions, and 2 have been referred to OGC for guidance where an ISO exemption was not appropriate. OGC anticipates that continued OGC support and analysis will help the field resolve or put the remaining 3 contracts into resolvable status regarding the necessary security measures; the remaining contracts constitute .00013 percent of the overall 22,000 contracts and agreements VHA analyzed to incorporate the VAAR Security Clauses. With continuing OGC support, that number may be reduced to zero. OGC staff had anticipated that the number of affected contracts and agreements would be reduced as further examinations showed the clauses would not be universally applicable to all agreements. Some contractors had needed VA staff to explain that they were entitled, pursuant to the Changes Clause of the contract, to be compensated for costs incurred but not anticipated for additional capital outlays for security measures, or that the contracts/agreements could incorporate the clauses as no-cost modifications.

OGC guidance and analyses have focused on helping VA procurement and ISO staffs to determine whether or not the third party involved needed to use, store, modify, generate, or transmit ***VA SPI*** or whether the third party (a) generated ***its own*** data or SPI, placing such agreements outside the scope of the VAAR Security Clause coverage, or (b) did not use, store, modify, generate, or transmit VA SPI in order to provide the services and supplies required or to perform contractual obligations for VA.

The ISOs, POs, and COs in the field are aware OGC will help them determine whether the clauses belong in a given agreement or situation, or, how they may work with contractors to understand and to use the clauses.

Question 10: Given the concern that there should not be a reduction in services to our Veterans, please respond to the following questions:

Question 10(a): Please provide the Committee a list of 579 contractors who refused to sign the information security clause.

Response: Attachment A contains the list of 45 contractors who refused to sign the information security clause as of June 9, 2010. The list was compiled after reviewing the 579 contracts which did not include the signed information security clause.

Question 10(b): How many of these contracts are currently providing critical Veterans' services?

Response: Of the vendors refusing to sign, almost all provide critical Veterans' services. Those vendor contracts not related to critical service are being reviewed regarding the applicability of the clause to the contract. COs working with the ISOs and POs, are reevaluating the contracts in light of the new guidance. This guidance consists of VA Handbook 6500.6 *Contract Security,* dated March 12, 2010, and the May 18, 2010, VAAR Security Clause in Contracts Memorandum from the Deputy Under Secretary for Health for Operations and Management.

Question 10(c): What will happen to the contracts if the vendor continues to refuse to sign the information security clause?

Response: The Veterans Health Administration (VHA) has been working diligently with several elements of VA, including OGC and the Privacy Office, to determine what steps should be taken when a vendor refuses to sign the VAAR Security Clause. VA has, as of May 19, 2010, received further guidance as to the applicability of the VAAR clause to nursing homes and other situations in which the vendors were refusing to sign. Guidance was provided by OI&T on March 12, 2010, as to the process in regards to obtaining clarity on when the clause is required in a contract. Our COs are currently working through those issues and have contacted their local ISOs and Privacy experts to identify if the clause is needed for these particular contracts. If it is, the CO will work with OGC to develop instructions on how to proceed.

Question 10(d): Will services to our Veterans be undermined if VA actively pursues these contractors or discontinues business with them?

Response: Yes. Many of these contracts are affiliate agreements that provide critical care necessary to serve our Veterans. Other contracts are service agreements to work on essential equipment that is needed to diagnose and treat patients. Attempting to cancel these contracts will be detrimental to our ability to care for our patients.

Question 11: Both the VA OIG and the GAO had identified areas of weakness at the VA relating to information security, particularly in the areas of access controls, configuration management, segregation of duties, contingency planning, and security management. What steps are being taken by the Department to address these deficiencies? Please provide the Committee with a timeline for full implementation of these measures.

Response: VA has made progress in addressing its material weakness related to information security. This approach is both reactive and proactive whereby it is focused on the remediation of existing vulnerabilities as well as significantly reducing the risk of future vulnerabilities across VA's information system infrastructure. VA's material weakness in information security is broken down into five primary components. These components, the progress made in each, and the estimated timelines for their remediation are shown below:

1. *Security Management* (Estimated Remediation Timeline: June 2011)

VA has made significant improvement in the development and management of its information security program. However, actual progress in eliminating the material weakness will not be known until November 2010 when the annual report comes from the IG. At this time, notable improvements include the following:

- *Centralized Management.* Increased accountability and standardization throughout the VA enterprise, the management of VA's information technology program and corresponding information security program were consolidated under the Chief Information Officer and Chief Information Security Officer, respectively.
- *Remediation of IT Security Weaknesses.* In FY 2009 alone, the VA closed more than 9,000 POA&Ms information security weaknesses, significantly reducing the risks to VA. To more strategically and centrally manage the Department's POA&M process, VA established several dashboards to visually represent the status of POA&Ms. VA strategically tracks and manages POA&Ms through its Security Management and Reporting Tool (SMART) database.
- *Risk Assessment.* VA improved the risk management of its information security program by establishing a new manual risk assessment process that is aligned with the steps contained in NIST SP 800–30, *Risk Management Guide for Information Technology Systems.* The descriptions of security controls that exist within major applications and general support systems have been enhanced and control enhancements are identified for controls viewed to be deficient.
- *Incident Response.* Through the use of new tools and technologies, VA has increased the timeliness and effectiveness of its responses to security incidents. Most notable is the use of the Formal Event Review and Evaluation Tool (FERET) which is an enterprise-wide tool that is used for accurate identification of data breach-related events and incidents which provides a quantifiable classification of data breach incidents by type and risk. VA uses FERET to prioritize data breach incidents (1) so that they can be addressed and corrected in a timely fashion and (2) to run trending reports to stay aware of and prevent recurring problems.
- *Certification and Accreditation.* VA has successfully certified (tested) and accredited (authorized for operation) more than 600 information technology (IT) systems. Certification and accreditation provides VA executives with a clear picture of the full extent of risk across all systems and a clear baseline upon which to build its information security program.
- *Continuous Monitoring.* VA performs continuous monitoring of its systems to help ensure that security controls are properly implemented. Continuous monitoring, which is part of Certification and Accreditation, encompasses a review of a subset of the system's overall security controls in order to ensure that POA&M items are appropriately addressed. VA also established an Emergency Response Testing (ERT) team as part of its continuous monitoring program. The ERT team scans the VA network for vulnerabilities to allow VA to proactively test for security weaknesses and correct deficiencies where necessary. This helps VA to reduce system security risk.

2. *Access Controls* (Estimated Remediation Timeline: October 2012)

While much work remains to be done, VA has made progress in strengthening the controls over access to its information and IT systems. Some of the progress which has been made to date is shown below:

- Deployed antivirus and host-based intrusion detection capabilities on over 200,000 endpoints with centralized management capability
- Implemented solutions for (1) the time-out of remote access and (2) the RESCUE initiative which provides a secure remote access capability to the VA enterprise
- Achieved over 85 percent compliance with all Trusted Internet Connection (TIC) requirements which are designed to reduce the number of external connections, including Internet points of presence
- Implemented Rights Management Service for Document and Email Security
- Employing mechanisms to ensure VA password complexity standards are enforced on all systems across the enterprise
- Continuing to provide laptop encryption for the mobile workforce with 30,000 devices encrypted and evolved encryption to include research and other non-laptop high-risk devices
- Completing implementation of virtual local area network (VLAN) controls to appropriately restrict access to sensitive network subnets at VA Medical Centers

3. *Segregation of Duties* (Estimated Remediation Timeline: March 2011).

VA is conducting periodic reviews of user accounts to determine whether access to VA information systems is not only commensurate with each user's job responsibilities but is also properly segregated to not allow individuals to compromise the system or its transactions. Since segregation of duties is both a security and a business risk, OI&T is teaming up with VA business lines to do these reviews. Adjustments to system access are being made, as appropriate, after these reviews have been completed.

4. *Configuration Management* (Estimated Remediation Timeline: July 2011)

VA drafted VA Directive 6004, Change, Configuration, and Release Management Programs, to establish Department-wide configuration, change, and release management programs in compliance with the Federal Information Security Management Act (FISMA) and has developed three Standard Operating Procedures/Guidelines that outline the procedures for each program. These documents apply to all VA-related components and IT resources, including contracted IT systems and services.

VA also established the Enterprise Security Change Control Board in January 2004 in order to ensure that all proposed changes to VA IT systems are reviewed, are viable, and will not adversely affect the operation of the existing system or subsystem. The Board is composed of operations, security, and privacy representatives who review proposed system changes for compliance to existing laws, regulations, and VA policies.

To better secure its information systems, VA developed the VA Federal Desktop Core Configuration (FDCC) settings for Windows XP and Windows Vista. These standards drew from the original Windows XP and Vista FDCC settings issued by NIST on July 31, 2007; those settings were then adjusted to fit the VA environment.

In compliance with the FISMA requirement to provide "policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency," VA also developed a set of minimum security configuration standards for Windows Server 2003, Apple/OSX, AIX, and Open VMS in order to ensure the other common operating systems and applications are securely configured. VA uses these standards in conjunction with the VA FDCC settings.

5. *Contingency Planning* (Estimated Remediation Timeline: September 2011)

VA developed a continuity of operations plan for the Office of Information and Technology to ensure continued IT support in the event of a crisis. In addition, VA has begun a concerted effort to not only test but document the results of contingency planning testing for it's over 600 IT systems.

○