OVERSIGHT HEARING ON VETERANS BENEFITS ADMINISTRATION DATA SECURITY

JOINT HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON ECONOMIC OPPORTUNITY AND THE SUBCOMMITTEE ON DISABILITY ASSISTANCE AND MEMORIAL AFFAIRS

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 20, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-54

28.450.PDF

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON VETERANS' AFFAIRS

STEVE BUYER, *Indiana, Chairman*

MICHAEL BILIRAKIS, *Florida*
TERRY EVERETT, *Alabama*
CLIFF STEARNS, *Florida*
DAN BURTON, *Indiana*
JERRY MORAN, KANSAS
RICHARD H. BAKER, *Louisiana*
HENRY E. BROWN, JR., *South Carolina*
JEFF MILLER, *Florida*
JOHN BOOZMAN, *Arkansas*
JEB BRADLEY, *New Hampshire*
GINNY BROWN-WAITE, *Florida*
MICHAEL R. TURNER, *Ohio*
JOHN CAMPBELL, *California*

LANE EVANS, *Illinois, Ranking*
BOB FILNER, *California*
LUIS V. GUTIERREZ, *Illinois*
CORRINE BROWN, *Florida*
VIC SNYDER, *Arkansas*
MICHAEL H. MICHAUD, *Maine*
STEPHANIE HERSETH, *South Dakota*
TED STRICKLAND, *Ohio*
DARLENE HOOLEY, *Oregon*
SILVESTRE REYES, *Texas*
SHELLEY BERKLEY, *Nevada*
TOM UDALL, *New Mexico*
JOHN T. SALAZAR, *Colorado*

JAMES M. LARIVIERE, *Staff Director*

SUBCOMMITTEE ON ECONOMIC OPPORTUNITY

JOHN BOOZMAN, *Arkansas, Chairman*
RICHARD H. BAKER, *Louisiana*
GINNY BROWN-WAITE, *Florida, Vice Chairwoman*
JOHN CAMPBELL, *California*

STEPHANIE HERSETH, *South Dakota, Ranking*
DARLENE HOOLEY, *Oregon*
LANE EVANS, *Illinois*

MICHAEL F. BRINCK, *Subcommittee Staff Director*

SUBCOMMITTEE ON DISABILITY ASSISTANCE AND MEMORIAL AFFAIRS

JEFF MILLER, *Florida, Chairman*
JERRY MORAN, *Kansas*
JEB BRADLEY, *New Hampshire, Vice Chairman*
GINNY BROWN-WAITE, *Florida*

SHELLEY BERKLEY, *Nevada, Ranking*
TOM UDALL, *New Mexico*
LANE EVANS, *Illinois*

PAIGE MCMANUS, *Subcommittee Staff Director*

CONTENTS

June 20, 2005

OPENING STATEMENTS

STATEMENTS FOR THE RECORD

WITNESSES

MATERIAL SUBMITTED FOR THE RECORD

POST-HEARING QUESTIONS FOR THE RECORD

Written committee questions and responses from Ronald Aument, Veterans Benefits Administration, U.S. Department of Veterams Affairs:

Written committee questions and responses from Michael Staley, Office of Inspector General, U.S. Department of Veterams Affairs, July 12, 2006, letters:

Written committee questions and responses from Linda Koontz and Gregory Wilshusen, U.S. Government Accountability Office:

OVERSIGHT HEARING ON VETERANS BENEFITS ADMINISTRATION DATA SECURITY

TUESDAY, JUNE 20, 2006

U.S. House of Representatives,
Subcommittee on Economic Opportunity,
Subcommittee on Disability Assistance and
Memorial Affairs,
Committee on Veterans' Affairs,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:00 a.m., in Room 334, Cannon House Office Building, Hon. Jeff Miller [chairman of the Subcommittee on Disability Assistance and Memorial Affairs] and Hon. John Boozman [chairman of the Subcommittee on Economic Opportunity] Presiding.

Present: Representatives Miller, Brown-Waite, Boozman, Berkley, Udall, Herseth, and Hooley.

Mr. Miller. Good morning everybody. This joint hearing of the Subcommittees on Disability Assistance and Memorial Affairs and Economic Opportunity will come to order.

I would like to begin by saying this morning that while testimony was due to the Subcommittees by June 16th, we did not receive the VBA statement until last night. We realize the Committee has scheduled a number of hearings this month. However, we gave plenty of notice, in my opinion, and receiving the testimony the night before a hearing does not serve us well in our oversight capacity.

On the 22nd of May Congress and the public were informed that several weeks earlier there had been a severe data breach containing sensitive information on more than 26 million beneficiaries. We learned just last week that an additional 2.2 million active duty servicemembers, reservists, and guardsmen and women may be affected as well.

Through testimony and briefings it is apparent that the Department's lack of specific policies and procedures has created security vulnerabilities. While none of us could have imagined a situation affecting so many millions of people, I am beginning to believe something like this was bound to happen.

Since becoming chairman of this Subcommittee, a common thread is emerging. There appears to be a lack of uniformity within the Veterans Benefit Administration and certainly among the VBA. Please understand that I'm not criticizing any single person or office. There is certainly a cultural mentality that exists in many bureaucracies. One of the difficulties facing a large agency like VA is that it takes time, it takes money, and buy-in to change that culture. VA has not always been the most effective in keeping up with changing technologies, models or demands. What has recently occurred has been the product of that resistance to change.

Whether it is lack of uniformity with how regional offices respond to a veteran or congressional inquiry, how claims are prioritized, or how information and technology and data security procedures are implemented, everyone seems to do things differently.

The IG found data security deficiencies at 37 of 55 regional offices. Now if 37 regional offices have 37 different ways of doing business, that requires a lot more management muscle to correct a deficiency than if we have a uniform implementation of procedures.

In order to receive benefits and services from VBA, veterans and survivors must provide at a minimum full names, social security numbers, and a home address. In order to receive benefits such as nonservice-connected pension, wage and other financial information must also be submitted.

All of us trust that the federal government will do everything in its power to safeguard the information that has been provided. Thankfully, we have not yet heard of any reports of identity theft, but the trust placed in VA has certainly been broken.

Our two subcommittees are holding this hearing to learn more about VBA's data security management program, what steps have been taken to educate its employees and how it intends to move forward to improve its data security policies. I do look forward to hearing from the witnesses that are here today, and I want to turn now to the chairman of the Economic Opportunity Subcommittee, Dr. Boozman, for his opening remarks.

MR. BOOZMAN. Thank you very much, Mr. Chairman, and I certainly appreciate your leadership in this area.

We appreciate you all being here. You will notice that we have a large print version that shows the 16 IT vulnerabilities cited by the VA Inspector General as yet to be addressed by the Department. The list shows a range of potential sources of data loss or compromise. The recent loss of over 26 million veterans personal data highlights several things.

First, data security must be founded on laws and regulations that are dynamic and enforced. Second, the appropriate technologies must be in place to implement the right levels of security and assist in enforcement and prevention. And third, there must be aggressive

and consistent enforcement by senior VA officials.

I do not know the motivation of the employee who willfully disregarded whatever rules were in place regarding working on the sensitive data from home, but what I do know is the VA missed an opportunity to increase its corporate control over data by imposing the bipartisan legislation passed by the House during the first session. That bill, H.R. 4061, would reform the way VA structures its management of its information technology programs. Without a solid foundation, whether in a building or an organization, everything above it is suspect. The policies at H.R. 4061, if put in place, would have provided that foundation. And while H.R. 4061 alone would not have prevented what has happened, if adopted, the VA would have had the basis for a coherent technology development and management program.

That would enable leadership to implement and enforce a whole range of policies designed to control not only the fiscal issues but also things like data security in combination with aggressive technical security applications. H.R. 4061 is the right answer at the right time and place. The Department should reconsider its position on this bill and move quickly to consolidate its information technology programs.

I am not just worried about cyber security. I am also concerned about how programs like vocational rehabilitation and employment control access to veterans papers at the regional offices and their contractors. These files often contain very sensitive psychological and other medical data which, if accessed by unauthorized personnel, could have serious consequences.

The constant theme in the testimony presented by the IG and GAO is the need for centralized cyber security among other things. If the VA refuses to adopt a centralized approach to managing its IT systems as prepared by H.R. 4061, how can you expect to achieve consistency throughout the VA system on anything related to IT.

While we are talking about consistency, I want to broaden the scope just a little bit. We constantly hear about how each regional office has its own process for handling benefits and that the first thing newly trained staff returning from something like Challenge Training is, "We don't do it that way in this RO."

It seems there is a lack of will by VA headquarters to impose and enforce best practices throughout its field operations. Everything seems to be a suggestion and is left to the RO director to choose whether or not to follow a policy.

While I may be overstating the case slightly, it is a real problem facing the Department and certainly this is a tremendous challenge. It is something that we as a committee are committed to helping.

Thank you very much, Mr. Chairman.

MR. MILLER. Thank you very much, Dr. Boozman.

I would like to now recognize the Ranking Member of the Subcommittee on Disability Assistance and Memorial Affairs, Ms. Berkley, for an opening statement.

MS. BERKLEY. Thank you, Chairman Miller and Chairman Boozman, for holding this hearing.

Since the Under Secretary for Benefits is responsible for information security at the Veterans Benefits Administration Office, I for one would like to understand what problems exist and the steps that are being taken to address these problems.

Veterans and service members in my district, I can tell you -- and I assume throughout the United States, are rightfully outraged that the security of their personal data has been compromised by the Department of Veteran Affairs, and I can assure you right after this was disclosed my phone in my district office was ringing off the hook and the level of anger and concern was very concerning to me.

In 2004, during a routine review by the Inspector General of the Reno, Nevada VA regional office, several deficiencies related to Benefits Delivery Network computer security and sensitive claims folders were identified. Similar deficiencies have been identified throughout the Nation.

The Inspector General has reported that although the VA is responsible for promptly correcting identified deficiencies, there is no systematic action taken to assure that the deficiencies identified in one office aren't corrected at other offices. This piecemeal approach to fixing problems probably provides little assurance to our Nation's veterans and probably isn't a very effective way of conducting business.

I am also concerned that there may be inadequate staff to perform audit functions at data centers. I am sure there is inadequate staff. In addition, it is not clear there is any method for assuring security and control of data extracts provided to various components of the VA. Extracts such as these were reportedly the source of the recent data theft.

I hope -- and I am looking forward to hearing what the witnesses have to say, but I hope that you will address these concerns. And again, thank you for being here today. I am looking forward to your testimony.

Thank you.

MR. MILLER. Thank you, Ms. Berkley. And now the Ranking Member of the Subcommittee on Economic Opportunity, Ms. Herseth.

MS. HERSETH. Thank you and good morning to you, Chairman Miller, Chairman Boozman, and of course Ranking Member Berkley and other colleagues. I am pleased we are holding this hearing today to review the procedures at the Veterans Benefits Administration and the efforts to control and maintain veterans' personal and sensitive

information in a secure manner. I welcome witnesses on both panels this morning. We appreciate your testimony.

The topic of today's hearing is both important and timely given the recent loss of nearly 26.5 million veterans' and active service members' private information. Indeed, the Federal Government, as a whole, every federal agency and the VA specifically, must improve its data security measures and enhance its recognition of and respect for citizens' privacy and health information laws, and it is incumbent upon us as a subcommittee, as a full committee, and the other committees on which we serve to ask these questions and to get the answers that will guard us as well in the future as it relates to the resources that each of our federal agencies need and the continuity of each CIO organization and the strength of those organizations to implement what we passed 10 years ago to ensure the data security of citizens' privacy and other information.

I have a chance to see a lot of veterans across South Dakota; in particular, a lot of our Vietnam veterans as we get ready for a Memorial dedication in Pierre, South Dakota this fall, and as we know, it took a number of those veterans sometimes a number of years to overcome a level of distrust to even reach out to the VA to obtain some of the benefits that they deserve and many of them that I see now just shake their heads when they received the information that their information was compromised.

And in addition to that, many of them are serving to reach out to newly returned veterans, to work with them to make the adjustment back home after their deployments, and all of these men and women deserve our very best. We know that the employees at the VA feel the same, but we have to ensure levels of accountability and a system that is in place with policies and supervision and enforcement to maintain the integrity of this data and a fast changing financial services environment.

So today, I am particularly interested in hearing about VBA's data security procedures with respect to information transferred to and from other Federal agencies, when information is controlled by contractors, such as the case when service members apply for education benefits or when contractors provide for vocational rehabilitation and employment services to a disabled veteran.

So both chairman, ranking member, thank you again for the hearing today. We look forward to the testimony.

MR. MILLER. Thank you very much.

The first panel is already seated at the table. Mr. Ronald Aument is Deputy Under Secretary for Benefits at the Veterans Benefits Administration. He is accompanied this morning by Mr. Jack McCoy, Associate Deputy Under Secretary for Policy and Program Management; Mr. Michael Walcoff, Associate Deputy Under Secretary for Field Operations; and Mr. Thomas Lloyd, Deputy Chief Information

Officer at VBA.

Mr. Aument, you may begin.

STATEMENT OF RONALD R. AUMENT, DEPUTY UNDER SECRETARY FOR BENEFITS, VETERANS BENEFITS ADMINISTRATION, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY JACK McCOY, ASSOCIATE DEPUTY UNDER SECRETARY FOR POLICY AND PROGRAM MANAGEMENT, VETERANS BENEFITS ADMINISTRATION; MICHAEL WALCOFF, ASSOCIATE DEPUTY UNDER SECRETARY FOR FIELD OPERATIONS, VETERANS BENEFITS ADMINISTRATION; AND THOMAS LLOYD, DEPUTY CHIEF INFORMATION OFFICER, VETERANS BENEFITS ADMINISTRATION

MR. AUMENT. Thank you, Mr. Chairman. Chairman Miller, Chairman Boozman and members of the subcommittee, thank you for the opportunity to appear before you today to discuss data security and the Veterans Benefits Administration.

I would like to open up with an apology for the lateness of our prepared statement, Mr. Chairman. I have no excuse for that.

I am accompanied by Mr. Jack McCoy, the Associate Deputy Under Secretary for Policy and Program Management, Mr. Mike Walcoff, Associate Deputy Under Secretary for Field Operations, and Mr. Tom Lloyd, Deputy Chief Information Officer.

With the committee's permission, I will offer a summary statement this morning and request that my written statement be submitted for the record.

MR. MILLER. Without objection.

MR. AUMENT. Let me assure the subcommittee that VBA is thoroughly examining every aspect of our information security programs, our processes and our procedures to ensure that sensitive veterans data is neither mismanaged nor used for any unauthorized purpose. Although our review is ongoing, I will outline security measures we have had in place prior to May 3rd, 2006 and additional steps we have taken regarding our data security policies and procedures. I will also specifically address the security of the data feeds between VBA and the Department of Defense.

Responsibility for all IT security policy is centralized to the Department's Office of Cyber and Information Security, which reports directly to the VA's Chief Information Officer. Implementation of IT security policy and procedures in VBA is through a three-layer organizational assignment of responsibilities. The Information Security Officer at each regional office is responsible for the execution and oversight of IT security policy and procedures. ISO has managed local access control to IT resources. It conducts security audits under

the focal point for incident reporting in the VBA facility. The network support centers provide oversight of regional office compliance of IT security policy and procedures and expert advice to the regional office ISO community and IT staff on technical issues. The VBA IT organization and headquarters provides technological support which implements IT support and procedures on the computer applications and systems.

The Secretary's recent decision to further centralize all IT operations and maintenance activities brings all of the VABs under the Department CIO. We believe this further centralization of IT security will raise the organizational focus on the critical security issues and challenges and will bring added oversight and safeguards for sensitive information and records. VBA has incorporated security into all of our information systems and benefits delivery processes. We have extensive well-articulated policies and procedures governing access requests, auditing and rules of behavior. These policies and procedures pertain to all VBA employees as well as any other individuals authorized access to VBA systems and data. In all VBA's benefit systems veteran data is protected by VA and VBA security policy and IT system and application security controls. Programmatic access controls restrict access according to the specific veteran's record level of sensitivity and the authority of the individual accessing the data.

All individuals authorized access to VA systems must adhere to rules of behavior that govern the use of IT systems and capabilities. The rules of behavior ensure that all users of IT resources are aware that any source potentially contains valuable and sometimes sensitive government or personal information which must be protected to prevent disclosure, unauthorized change or loss.

The VBA internal controls process requires regional office directors to conduct systematic analysis of their IT security operations and to certify annually that their facilities are in compliance with the directives. The network support centers conduct annual surveys to ensure that the ROs are adhering to all VA, VBA and all other Federal security directives in the handbooks and that the deficiencies identified through the Inspector Generals combine that assessment program reviews are remediated.

In August of 2005, VBA completed the federally mandated certification and accreditation of 97 application systems on schedule. VBA has a secure technology solution in place for external system users. External access to VBA is controlled through the One-VA Virtual Private Network to a centralized terminal server. VBA outbased workers as well as authorized veteran service organization representatives used One-VA VPN capability. Additionally, the Veterans Administration Portal supplies secure encrypted user access to loan guarantee applications for internal and external users.

In March of this year we started the process to accelerate the imple-

mentation of public key infrastructure technology throughout VBA. PKI will provide a common utility for VA to provide more secure electronic transactions and e-mail. VBA is supporting the Secretary's direction to accelerate to annually require privacy awareness and Social Security training. All VBA's employees are now required to complete these training programs by June 22nd. That will be this Thursday.

We have compiled a list of VBA databases that contain sensitive information and all interfaces or data feeds that update these database. A VBA work group has been tasked with assessing all VBA policies and procedures related to the release of data protected by the Privacy Act to provide recommendations to improve protection of the data.

We also updated and strengthened procedures for handling veterans' requests to change address and direct deposit information to ensure proper verification of identity of the individual requesting the change. In the average month, we receive in excess of 40,000 requests from VA beneficiaries to change their financial institution and/or their address.

Effective June 7th, in accordance with the Secretary's direction, VBA suspended all work at home and Flexiplace arrangements for employees directly involved in disability claims processing. Employees who adjudicated claims at their homes or other non-VA work sites will now do all claims works requiring claims files in regional offices. While VBA evaluates various solutions to protect sensitive data transported to and from offices, we are also developing a standard work at home and Flexiplace agreement to ensure all employees absolutely understand the responsibilities to safeguard sensitive data.

VBA will implement VA encryption solutions. We have procured encryption capabilities for laptop computers and are considering expanding the use of the terminal server concept as a means of reducing or eliminating the information stored locally on a user's work station. We are also working with the Office of Acquisition and Material Management to reinforce strong control of the shipping of records containing personal identifiable information. This includes review of tracking procedures, signature requirements and expedited shipments. Department of Defense data is delivered to VBA via secured transmission using commercial software products and direct computer-to-computer connection. These tools are used when sending or receiving files from the Defense Manpower Data Center.

The VA is fully committed to the uninterrupted delivery of the benefits to those who have returned from the battlefield and who are transitioning into our VA system. We recognize the importance of securing the information shared with our DOD partners.

Our mission is to serve veterans and to provide benefits to the best of our ability. IT is an essential tool that helps us serve veterans better, faster and more thoroughly. However, the rapid rate of tech-

nological advances, while offering improved and expanded benefits delivery, also presents an ongoing challenge to VA to keep pace with security and privacy demands. IT can make our service better and faster but the vulnerabilities increase just as fast. We must and will do what is necessary to protect as well as serve our veterans.

Chairman Miller and Chairman Boozman, this conclude my statement. I will be happy to answer any questions you or any members of the subcommittee might have.

[The statement of Ronald Aument appears on p. 40]

MR. MILLER. I don't know how many hearings that I have attended, and there are more to come in regards to this particular issue. I know my colleagues have all been involved in hearings, and this is not a question that was prepared, but probably one that all of my colleagues want asked.

Every time I come into a Committee hearing where we are dealing with this issue, I am angry. More than angry. And then when I sit down and I hear the testimony that is given and the way the testimony is given and there is no emotion in the testimony, and I want to know what was your personal feeling when you heard that this had occurred.

MR. AUMENT. I felt somewhat betrayed that we had provided information to a trusted source that we expected to take the same level of care of that information that we would expect of our own employees and I felt betrayed and I felt as though we had betrayed our veterans.

MR. MILLER. I am glad you ended your statement with "we have betrayed veterans" because the employee doesn't matter to me. That employee is gone. And whatever reason, it's over. But I sat in here, I think it was last week, and listened to testimony and there is no visceral reaction that I can tell except the Secretary was shaking profusely because he was so angry when he testified the first time. But I don't see it from anybody else, and I hope that it is just me not reading people's body language correctly.

I would hope that everybody sitting at that table today would be mad as hell, and I don't see it. Can I ask the people who are with you if they are upset too?

MR. AUMENT. Of course.

MR. MILLER. Mr. Lloyd.

MR. LLOYD. Yes, sir.

MR. MILLER. Mr. McCoy.

MR. MCCOY. Absolutely.

MR. MILLER. Mr. Walcoff.

MR. WALCOFF. Yes.

MR. MILLER. Thank you.

Who at VBA is responsible for implementing the new directive that

is out there, Directive 6504, and how is it being implemented?

MR. AUMENT. Well, as with any directive, Mr. Chairman, the Under Secretary is ultimately responsible for its implementation. Directive 6504, and I may turn to my colleague, Mr. Lloyd is very much a technical -- has many technical capabilities, that we would rely upon the IT organization for its ultimate implementation.

MR. MILLER. Mr. Lloyd.

MR. LLOYD. With the implementation of the federated model the operations and maintenance people of VBA have been detailed to the CIO's office. We continue a close working relationship, and we are working to implement the directive. We have implemented the acquisition of the laptop software that Mr. Aument mentioned. We are working with the ISOs on our collection of information about who has access to every system, every application and the assurance that the documentation is appropriate for the access that the people have. We are looking at our databases, who has access for the appropriate approval and the documentation. We have developed a plan to implement all of the items in the Secretary's directive.

MR. MILLER. As a follow-on, 6,000 accredited VSO representatives are out there today but only 1,300 have completed the training responsibility involved in preparation of claims. How do you ensure and monitor that only registered users have access to the system and how does VBA monitor representatives as fiduciaries?

MR. AUMENT. The Veterans Service Organization representatives have to undergo the same types of training both in IT security and in privacy training that we require of any VBA employee. Anyone accessing the VBA system has to submit a request that at the local level those are managed by the ISO, the Information Security Officer. We also require that before anyone is given -- granted access to our systems in the VSO community that they would read, understand and sign the rules of behavior that we require of all VBA employees that we afford access to systems as well.

MR. MILLER. I may have a follow-up question that I will submit for the record. Another question that has been asked in other hearings is about the -- I guess it was in the mid-1970s C File numbers were used and then there was a transition to social security numbers. Are you exploring a change to the policy of using social security numbers?

MR. AUMENT. We have certainly discussed that. I know that is an idea that has generated a lot of interest from those concerned with this data loss. At the moment I believe that we are probably -- it is not a solution that we can take and run with, Mr. Chairman. We receive data importantly, most importantly from the Department of Defense, which uses as their unique identifier Social Security numbers for those transitioning from the military services. We are also required by law to provide extensive -- have extensive information exchanges with other government partners. By law, we are required

to do data matches with the Social Security Administration and the Internal Revenue Service to support the continuing payments of benefits to those individual unemployability or for means tested programs. We have to provide information through data matches to the Department of Education for veterans who are applying for assistance in the Department of Education programs.

This is just to mention a couple of the types of exchanges that we have to make routinely with outside interests in support of veterans programs.

These entities all use Social Security numbers as their unique identifier. So even if we for internal purposes decided to revert back to a unique claim number, we would still have to be able to cross-reference that in some fashion to Social Security numbers to facilitate these types of exchanges.

MR. MILLER. Thank you.

Dr. Boozman.

MR. BOOZMAN. Why don't I yield to the gentlelady from Nevada, and then you can come back to me.

MR. MILLER. I was going to do that, but then I was told protocol said I had to go to you first.

MR. BOOZMAN. You did go to me and I yielded.

MR. MILLER. Thank you. You are a kind gentlemen. You can be the hero.

MS. BERKLEY. Thank you all very much.

You know, it is -- how can I say this, I didn't have the same reaction that the chairman had about people not being mad enough because I didn't sense, quite frankly, that the Secretary -- he was mad but I think he was mad because this happened under his administration and frankly, if it hadn't blown up in everybody's face, I don't think -- I think he is so disengaged from the day-to-day operation of this department that he wouldn't have known, he wouldn't have cared, and he wouldn't have bothered to inquire.

But what I am always struck with when people from the VA come and talk to us is how great the policies are. And I mean you can, you know, we have heard testimony about some of the best policies and signing in and signing out and handbooks and all of the employees have training and yet the reality is that we have got a mess on our hands. So it doesn't matter much what our policies are. If they are not implemented and if we don't have people making sure that these are implemented, and I might be wrong, but I understand that the employee who is no longer here that the 26 or 27 million names were stolen from, he had done everything he needed to do, signed the -- signed whatever he needed to do, attended whatever seminars he needed to do and he went ahead and did something completely wrong for 3 years that he wasn't supposed to be doing. So it doesn't much matter what our policies are if we don't make sure that they are fol-

lowed.

Let me ask you a couple of questions, or I have a number of them but there may be a second round.

How are all of the regional offices notified of patterns of deficiency identified by the IG? I mean, is there a method of letting everyone know?

Mr. Aument. Yes, there is, Congresswoman.

Ms. Berkley. Do we do it?

Mr. Aument. Yes, we do. In fact, during the month of May, early in May, Admiral Cooper sent a memorandum to the regional officers bringing to their attention the deficiencies that were uncovered during the prior year's Inspector General CAP reviews. And I may ask Mr. Walcoff, my colleague, to discuss a little bit, you know, further about what the expectations are but --

Ms. Berkley. I would like to know once he sent out the notice in May, did we get feedback, do we know that they are now in compliance or moving towards compliance? How do we do this?

Mr. Walcoff. The letter that Ron was talking about was dated May 10th, was sent out by the Under Secretary, and we have gotten confirmation from every regional office that they are in the process of working on every one of these areas that was identified by the IG in their reviews, even in the situation where they themselves weren't reviewed but our OS officers were. So they were supposed to review their own office to make sure they don't have deficiencies in that area.

The IT recommendations will be fully implemented -- I think I gave them till Friday of this week. The non-IT recommendations they have another 3 weeks after that to fully implement, but we will get a certification from every regional office director that it is done in their office.

Ms. Berkley. Do you think you can provide us with a copy of that letter for the record?

Mr. Walcoff. Sure.

[The information appears on p. 100]

Ms. Berkley. How does VBA control data which is extracted from VBA's data system for use by a VBA office and other -- VBA's other departments?

Mr. Aument. Let me begin by giving you background and maybe transitioning into what we believe needs to be done as well.

Presently, any outside entity, and that could be both from within VA or from outside of VA, first has to initiate a formal request that goes to our Chief Information Officer within VBA. They conduct a technical review of that request for data and then they consult back to the program office responsible for the contents of that system; for example, that would include our compensation and pension service

or education service dependent upon the nature of the request, to try and make some determination of the appropriateness and the need for that request.

They then would, based upon that consultation, make a determination as to whether or not to provide that information.

At that point typically it has to go then to one of our data centers to have, you know, database administrators do the programming necessary to actually extract the data from the relevant system, and then it is made available based upon the requested arrangements with the requestor. That is quite a range of potential business partners that make use of that sort of information.

MS. BERKLEY. Do we have a log? How do we monitor this?

MR. AUMENT. Absolutely. There is a number of them that are routine data exchanges. We probably have some noted in the hundreds for that going to entities such as the Department of Defense, the Department of Education, other types of Federal partners as well as internal ones. Our Office of the Inspector General receives routine data extracts out of the compensation and pension system as well as from the BIRL system.

This is an area that we have charged our performance analysis and integration to do some additional due diligence on behalf of VBA. We believe that we need to have better rules on monitoring that. For example, better rules governing how that information can be used, better rules that would make sure that that is not shared with any other entity or reconstituted in any other fashion, better rules saying the duration which they are allowed to maintain that data. If it is given to them for a specific purpose, we believe an improved system would require what they must do with it after they have completed that task is to destroy it, return it back to VBA. We have looked at some other entities, Social Security, for example, that we believe serves as a much better model for that. And it is our intention to try to strengthen this process considerably.

MS. BERKLEY. Thank you. Are we going to have a second round? In that case, I will yield. Thank you very much.

MR. MILLER. Dr. Boozman.

MR. BOOZMAN. It is interesting, the VA, you all can be complimented, I think the system can be complimented in the sense that you have really been a leader in getting our records into format, which is important. This whole country is going through this transformation process to make it easier for people to get access and yet along with that we want the access where we can use these things and yet now -- and this is a huge thing that is something that again the whole country is struggling with how you protect access from unwarranted whatever.

So like I say, you have done a good job at switching over. That is to be commended. But I think the committee feels like you have

not done as good a job as we need to and certainly this new incident brings that to a head.

I mentioned in my opening statement that we passed H.R. 4061 to consolidate IT policy and system development under the corporate Information Security Officer.

In light of what has gone on and in light of showing some weaknesses in the system, is there any rethinking of your position on the bill? Is there any way we can work with you to --

MR. AUMENT. Well, Mr. Chairman, I don't speak for the Department in that regard. The Secretary certainly has made a decision as to the organizational change that he believes is needed and our job is to make sure that we implement the Secretary's decision as thoroughly --

MR. BOOZMAN. We can assume that is a no.

MR. AUMENT. Right. We certainly agreed, I think -- I mentioned that in my opening remarks, I think, that the IT security arrangements are going to be strengthened by the centralization of all security assets under the guidance of the CIO.

MR. BOOZMAN. Last week's full committee hearing GAO and VA's own Inspector General's Office doesn't give its Chief Information Officer authority to implement the recommendations without approval from 33 Under Secretaries. Do you believe that that is appropriate and that the Under Secretary should have that authority?

MR. AUMENT. Do I believe that is appropriate? I believe the General Counsel is reviewing that issue at the moment as we speak, and I am not sure that is an accurate statement today given the centralization of all of the security assets now to the CIO. It is my belief he has direct line authority today over all of the ISOs and all of the field personnel responsible for maintaining our systems.

MR. BOOZMAN. So the IG testified to that effect last week, so it is changed?

MR. AUMENT. Well, again, that is an area that is probably a little bit outside of my portfolio. But I do believe that with the detail of the personnel that are going to be permanently reassigned on October 1st that the CIO has direct line authority for all of the field IT staff within the Veterans Benefit Administration.

MR. BOOZMAN. But you would agree that makes sense to do it that way?

MR. AUMENT. Yes, I do.

MR. BOOZMAN. Do existing labor agreements contain any provisions for enforcing unauthorized use or access to data? If not, do we anticipate revising the labor agreements to enable the Department to hold employees accountable for these type of actions?

MR. AUMENT. Yes. It is not necessarily built into the labor agreement but our rules of behavior that every employee must sign it is explained in those rules of behavior that there are consequences for

violation of those practices and policies. It is explained to them. That range of consequence can be from terminating their access privileges to systems up to removal from Federal service.

MR. BOOZMAN. Could you give us copies of the rule?

MR. AUMENT. I would be happy to.

[The information appears on p. 107]

MR. BOOZMAN. Thank you, Mr. Chairman.

MR. MILLER. Ms. Herseth.

MS. HERSETH. Thank you, Mr. Chairman.

MR. AUMENT, I notice on your written testimony on page 10, actions taken to inform veterans about the data theft, that you talk about public contact teams working extended hours contracting with GSA, meeting with other contractors. I am somewhat familiar with what GSA charges our Federal judges and their chambers to rent space and provide other services. So can you tell me how much the VA has expended on notices to veterans operations to call centers and other activities related to the data breach and from what accounts the funds are being provided?

MR. AUMENT. I certainly can, Congresswoman. Let me begin with the mailings, the direct mailings that have been made to veterans and service members to inform them of this data breach. A total of 17-1/2 million letters were sent out in this first round of mailings. The cost for that was over $7 million. Around a million dollars cost for the printing costs and somewhat over $6 million for the postage cost of that mailing.

For the call centers, we have spent to date the last I was informed on this was 3 to 4 business days ago we had spent slightly over $7 million for the operations of the call centers. And that we are probably spending today a little bit over $200,000 a day for their continued operation.

That money at the moment I must say is not strictly a VBA expenditure but departmental expenditure in that they had made arrangements with the Appropriations Committee for reprogramming for other funds to support this effort.

MS. HERSETH. And are the mailings coming out of -- you said the first round of mailings. Is it coming out of VBA or --

MR. AUMENT. We are anticipating there may be follow-up communications that are warranted on whatever types of follow-up actions that the administration and Congress feel may be needed to help veterans in this matter.

The compromised information came from the BIRL system. I am sure you have seen referenced in some of the explanations here -- contains -- not contain veterans addresses. So we really did not know the addresses of these individuals, many of whom are not receiving benefits from VA.

We obtained -- we did not really even obtain those addresses, but we had to send data or our data files to Social Security Administration who reviewed through their records to try to find valid addresses and Social Security numbers. They did some Social Security number validation on that. They in turn shared the information with the Internal Revenue Service to try and find as many accurate addresses as could be possible from those data files. Then that information was then passed along to contractors to the Government Printing Office. But none of that information actually came back to VA.

MS. HERSETH. Okay. I think I followed the circuitous route that this took.

So you mentioned that there has been a request to the Appropriations Committee both for fiscal year 2006 and fiscal year 2007 and reprogram moneys.

MR. AUMENT. Not fiscal year 2007.

MS. HERSETH. Do you think there will -- anticipate there will be a request?

MR. AUMENT. I really hate to speculate on that. I don't know of anything that is planned on that at the moment.

MS. HERSETH. Along the lines of what VBA understands to be within this universe of compromise data, let us say hypothetically -- well, let me first ask the question of the 17-1/2 million letters that have been sent, those have all gone to and what you just described there in trying to verify matching Social Security numbers up with addresses to those within the universe of the 26-1/2 million veterans whose data was compromised?

MR. AUMENT. Yes.

MS. HERSETH. If an active duty airman has only contact with the VA, has been to apply for a home loan, was he informed within -- I am still trying to understand who was really encompassed by --

MR. AUMENT. The process of information entering into that system today since the early 1990s, the Department of Defense has sent us information at the time of enlistment in the service, so that the service member need not have applied for any VA benefits to have had their information included in this system.

MS. HERSETH. And I know there will be a chance for a second round. So is the VA, VBA, everyone is still trying to figure out just how this universe came together with this particular employee's project that he was working on so it is more just what you had as of enlistment, but we still aren't quite sure how someone could have been drawn into that pool, that universe of individuals whose data was compromised? We are trying to figure that out?

MR. AUMENT. We believe we know the one large file that we are speaking of, this extract from BIRLS. We understand the programming that was used to select the records that went into that. So we believe we understand the universe of compromised records.

The 26-1/2 million, it is the difference between 26-1/2 million records versus the 17.5 million records was sent out, was that not all of those records contained all of the complete data. For example, I ran 7 million of those records, they contained no Social Security number. Without that Social Security number, it was not possible to conduct any sort of accurate address determination on that.

So we also found that in the records, included in the records were invalid Social Security numbers in some cases, which once again would have prevented any sort of a finding of address, and in some cases it involved deceased veterans as well.

MS. HERSETH. I will wait for the second round. Thank you, Mr. Chairman.

MR. MILLER. Ms. Brown-Waite.

MS. BROWN-WAITE. Thank you very much, Mr. Chairman. In reading over the testimony, it was noted that VBA has recalled all work-at-home employees and required them to return all files and equipment to VBA. How do you know what files they have?

MR. AUMENT. I am probably going to turn this over to Mr. Walcoff, but there have always been in existence for all of our claims adjudicators who are working at home fairly rigid check-out/check-in practices for any files that they take away from the regional office, you know, for work home -- under work-at-home agreements.

MS. BROWN-WAITE. Do these include electronic files? If they downloaded an electronic file, what record do you have of that? And I will let the gentleman answer.

MR. WALCOFF. Well, the --

MR. MILLER. If you pull your mike and then turn it on.

MR. WALCOFF. The vast majority of the work-at-home people were rating specialists and we have -- we use a system called COVERS to electronically track where a folder is so when they take folders home, we will wand it and it will be electronically recorded that that folder is being taken home by that particular rating specialist. So we are able to make sure that every folder that was taken out by our rating specialist back to his house was brought back when he brought all of the equipment in and all of the hard copy folders.

MS. BROWN-WAITE. I am not sure that I got the answer to the electronic files.

MR. AUMENT. We may have to turn to Mr. Lloyd on that. But I believe that the on-line components of the veterans' record are not downloadable to these individuals' work station. They would have the narrative descriptions of the rating decisions that they are working on for the immediate case that they are working on on the personal computer. But --

MS. BROWN-WAITE. I would also ask what COVERS, the acronym, what that stands for?

MR. AUMENT. I am not sure, Congresswoman. It is the tracking

system that we use internally and externally in the regional office to track the locations of veterans' claims folders.

MS. BROWN-WAITE. Is that the same system that when I call in on behalf of a veteran that the file could never be found?

MR. AUMENT. I am not really able to answer that question.

MS. BROWN-WAITE. Or is that another acronym?

MR. AUMENT. Could you restate the question, please?

MS. BROWN-WAITE. Is that the same system that when I call in inquiring on behalf of a constituent that the file can't be found, is this the same system?

MR. AUMENT. Quite possibly, yes. The difficulty there would be within the regional office we could identify it is within the service center but as to whether or not it is on an individual's desk or on a file cabinet sometimes it might be imprecise in that fashion. We would be able to track if it has left the building under the work-at-home program.

MS. BROWN-WAITE. I still need the answer to the electronic files question.

MR. LLOYD. When a veteran rating specialist works at home, they take the folders with them and they use an application called RBA 2000. That application allows them to work at home in the development of their rating information. There is a local database on the PC they use at home that contains the work that they are doing while they are at home. When they come back to the office, which I believe is weekly or biweekly, they upload that information into the corporate database. So while they are working at home there is information in the development of the ratings that they are doing.

MS. BROWN-WAITE. Just a follow-up question, Mr. Chairman.

When you ask them to return all files and equipment, what sanctions were there if this request was ignored?

MR. AUMENT. There were 370 ratings specialists in total working from their homes who were required to return to the regional offices. I believe that involved most, if not at all regional offices.

Mike?

MR. WALCOFF. Yeah. Not every station had work at home -- had people working at home. I would say about two-thirds of the stations did and every one of them has come back to the office with their equipment, with their files.

MS. BROWN-WAITE. One other question.

On page 13 of the testimony of Mr. Aument, there was a statement that said VBA -- it is about, almost halfway down the page -- information security officers are required to review users' access and privileges at least quarterly or when a job change occurs.

ter a job change occurs, how soon does that review take place, you know, and you know job change could be termination?

MR. AUMENT. Tom, do you have an answer to that?

MR. LLOYD. Specifically for the terminations part of the check-out procedure, the supervisor and HR staff are to inform the Information Security Officer that the employee has been terminated and the ISO is supposed to remove all permissions and access on the day that the person leaves. That is the process.

MS. BROWN-WAITE. Has there been any examples of when the access continued after the employee was terminated?

MR. LLOYD. I am aware over the course of the years where -- especially interorganizational terminations that we don't always inform each other and the ISOs didn't know an employee has been terminated.

MS. BROWN-WAITE. Has that situation been remedied?

MR. AUMENT. One of the things we are doing at the moment with Mr. Lloyd, an example that he might be referring to where a VHA employee has access to a VBA system, authorized access, and we may not follow as closely when that individual changes jobs, is reassigned, retires or is terminated. We are working with the Department for a solution on that today. That would allow us access to our payroll system to have these automatic updates provided from the payroll system to that effect.

MS. BROWN-WAITE. Just one quick --

MR. MILLER. Let's go to the other two members and then we will come back.

MS. BROWN-WAITE. Okay.

MR. MILLER. Did I hear you right that every file that is taken out or all information that is taken out you have the ability to track when the information leaves; is that true?

MR. AUMENT. All the files, you know, have a bar code attached to the file. The procedure is that when a file is -- it leaves the building under the work-at-home program would be to, you know, using the bar code reader check that file out and at the time it returns check the file back in.

MR. MILLER. But going back to Ms. Brown-Waite's question, that is not an electronic file, correct? That could be a paper file?

MR. AUMENT. That is a paper file.

MR. MILLER. So an electronic file could have been removed and you don't have a way to track that?

MR. AUMENT. We do not have all of the veterans' data -- I wish I could say otherwise -- contained in anelectronic file.

We know that. All Members of Congress are aware of that.

MR. AUMENT. Right. So that the information that they would have access to at home through RBA 2000 is the information accessible to them.

MR. MILLER. I guess I am still trying to figure out how we are still not sure today of the information that is missing, who it affects, and it seems like every week we get a new group of people that are included.

How is that so?

MR. AUMENT. I believe, and you will certainly have an opportunity to speak to the next panel, the Inspector General has been looking carefully as to what access to data this employee actually had. I would like to think that, you know, we know fully today and that there will be no further disclosures, sir.

MR. MILLER. Thank you.

MR. UDALL, questions?

MR. UDALL. Thank you, Mr. Chairman. According to the IG testimony, a contractor successfully penetrated the VBA system access to regional office files, created a fictitious veteran, established an award and mailed an award letter to a real address.

If all of the policies and procedures you described were in place and functioning, how was this possible.

MR. AUMENT. This incident, Congressman, took place a little over a year ago at our Waco regional office. Let me start to begin with, and I am sure you will follow up with our colleagues from the Inspector Generals Office, that first of all, they were already afforded access to the system. The IG had requested permission to get inside the firewall. So this did not replicate the situation where an entity outside VA would have broken into the system to have done this type of fraudulent activity.

MR. UDALL. Would somebody with the information that was taken out in the case of this recent employee, would they have been able to use that information and access the system?

MR. AUMENT. No, they would not have.

MR. UDALL. Go ahead.

MR. AUMENT. But the Inspector General was already given privileged status to be inside the system wherein they then conducted what is the equivalent of sophisticated hacking of captured passwords.

What this really demonstrated would be that a sufficiently skilled VBA employee with fraudulent intent inside a system, you know, could go ahead and have replicated the IG's efforts to create a fictitious payment. Now, they have identified to us the shortcomings, you know, the critical vulnerabilities and we have taken actions to address those vulnerabilities.

MR. UDALL. So from what you are saying then no longer would somebody within the system with the access they have be able to do what they did?

MR. AUMENT. I believe we have remediated. There was about a dozen different vulnerabilities they have raised. We have remediated most of those. Any of those who have not been completed, they are in the process of remediation.

MR. UDALL. According to the IG, VBA senior leadership is not receiving information concerning the financial costs of correcting conditions identified by the IG. How can VBA obtain a complete and

accurate picture of the resources and funding needed to remediate security deficiencies without such information?

MR. AUMENT. I am not really certain of what the IG's particular findings and recommendations are in that regard. I do know that one of the largest undertakings that we have begun over the past year was the completion of the original round of certification and accreditation of application systems that were completed by the end of fiscal year 2005. We have gone through and we have identified all the tasks that need to be undertaken to remediate the findings of that process, and we have attached a price tag to each and every one of those remediations.

We understand what it is going to cost us to solve those problems. Other types of problems that we believe that we need to be addressing, it is in a full encryption solution, both for, you know, desktop systems as well as the transmission systems and our legacy systems. We have attached price tags to those as well, too.

There may be some financial unknowns, but we believe that we have tried to address, get our arms around those as best as we possibly can.

MR. UDALL. According to your testimony, in the average month VA receives in excess of 40,000 requests to change the financial institution or address for receipt of benefits.

I understand that all financial institution changes for veterans being paid on Vets Net must be manually adjusted at the Hines BDN. Is this still the case and when will VetsNet be able to handle such transactions without manual rekeying of information?

MR. AUMENT. Tom, can you answer that? I am not sure that is still true or not.

MR. LLOYD. I believe, Congressman, that is in the August release. It is the issue of when they change from check to or from EFT to check.

MR. AUMENT. I see.

MR. LLOYD. And that is in the remediation that was --

MR. AUMENT. I don't know if you got that.

MR. UDALL. SO THEY ARE ABLE TO DO THAT NOW?

MR. AUMENT. They will be in August.

MR. UDALL. Thank you very much. Appreciate it.

MR. MILLER. Ms. Hooley.

MS. HOOLEY. Thank you, Mr. Chairman. I want to follow up on Ms. Brown-Waite's question.

I know that you stopped the work-at-home privileges. And a lot of those paper files had irreplaceable documents in it.

My question is when they took them home, they could, it seems to me they could take something out of that file and still scan it in. Are there backup copies of those documents? Are there electronic copies of those documents?

I don't think there is anyone in the room -- maybe there is someone here -- that hasn't at some point lost something out of some file. And so assuming that they didn't take them deliberately, maybe they just lost them. Are there backup copies of those documents.

MR. AUMENT. No, there are not, Congresswoman.

MS. HOOLEY. Is that changing?

MR. AUMENT. No, it is not.

MS. HOOLEY. Do you think it needs to be changed? If they have irreplaceable documents, don't you think you need a scan of those?

MR. AUMENT. I think we should ultimately move to an electronic record system. I could not agree more.

MS. HOOLEY. And when do you think you can move to an electronic system?

I mean, when you are dealing with that much paper, we have all, every single one of us here, every Member has known about cases where they can't find the files. They can't find the documents. But when are we going to get there?

Mr. Aument. In some of our program business lines we are already there. Our insurance program uses a totally electronic record, our education program uses electronic records, totally imaged files. The real challenge for us is our compensation and pension business line.

I would -- one of the places I would encourage you to visit, if you have an opportunity, is our Records Management Center in St. Louis. There are over 20 million files in that building that represent veterans' claims folders, as well as service medical records that we receive from the various military services.

The process of converting those files to either electronic images or, more importantly, data that can be used within the systems is a daunting challenge. We are attempting to tackle that in the pension component of the compensation and pension business line through our pension maintenance centers. They are moving to a totally electronic record, but we are not there yet, Congresswoman.

MS. HOOLEY. I saw the letter that went out to the veterans notifying them of that data breach. My question is -- I saw the letter and I didn't think the information in there was very useful about what to do. So my question is, now you have got the call centers, and you have got your employees. Have they been trained to handle questions from the veterans that come up in the process of their casework? Have they been trained to know what the answers are to the questions they ask?

MR. AUMENT. Yes, we have, Congresswoman. We have attempted to provide a set of -- I hesitate to use the word, but "scripts" or "answers to frequently asked questions" from concerned veterans. We have been providing those both to the contract call centers as well as to our public contact teams at our regional offices.

We are probably now on our fifteenth iteration of updating that

list of frequently asked questions, based upon our experience, coming in from concerned veterans and callers and their family members. So we have been doing our best to try and keep them informed with what we understand to be the types of questions most veterans are asking.

MS. HOOLEY. A couple of the most useful things I think you can tell the veterans is that they can put a fraud alert on their credit reports and they can get free credit reports, and yet when I went online after this happened, if you went through the whole system, you might get to that answer.

Are those kinds of things being told to the veterans now?

MR. AUMENT. Today, at the call centers and at our regional offices we attempt to respond to the questions. So if that question is posed, we certainly provide that information.

MS. HOOLEY. That question may not be posed because they may not know enough to ask that question.

MR. AUMENT. Correct.

MS. HOOLEY. It seems to me those are things that people should be told that they can do. They could be told immediately one way to help prevent identity theft, which is -- the whole idea behind this is to prevent identity theft, which is a very long, tedious process if that happens to you, that they can put a fraud alert on immediately, and that lasts for 90 days; and they can get a free credit report, which helps them keep track, to make sure nothing is happening to their account.

Why isn't that information given to them now?

MR. AUMENT. I think I mentioned, in response to Congresswoman Herseth's question about our mailings, that we are potentially contemplating a second mailing. Some of the drafts of communications I have read included precisely that sort of information.

MS. HOOLEY. Again, the letter is not being sent, but I would hope that at the call centers, that is information -- without them asking the question, that is information, here is what you can do.

MR. AUMENT. We will take that one on, Congresswoman.

MS. HOOLEY. Thank you.

MR. MILLER. We will go to a second round, and I would like to ask the members if you could ask just one more question to each person so we can move to the second panel.

To follow up on Ms. Hooley's question, when somebody puts a fraud alert on their credit file, do you know what the impact is to that file?

MR. AUMENT. I profess no expertise in that, Mr. Chairman. As far as -- I have seen some different iterations of the various levels of protections, just over the past couple of weeks, that can be involved and the terms of art that apply to a fraud alert versus a credit freeze versus something else. I know that there are various levels of protection afforded there. Some would require that the individual who

invokes that type of a credit check would ask to be contacted by one of the credit bureaus in the event that anyone attempted to obtain credit using that Social Security number.

We also understand that some of these types of provisions vary on a State-to-State basis as well, so that there are some differences based upon where a veteran may reside.

MR. MILLER. I think the thing that confuses a lot of us is that the mistake was made by VA, yet the burden has been placed on the back of the veteran. I am trying to figure out, why isn't VA being more proactive, other than sending out a letter, and if there is a way to make a mass notification to credit bureaus of the information, because you know who they are because you sent letters to them.

If it is not going to negatively affect them in one way or another and their ability to get credit or their borrowing power, wouldn't that be a responsibility of VA?

I mean, every time I hear VA talk about the issue, it is what the veteran can do to protect their identity. My God, they thought their identity was protected. VA screwed up and now we are putting the onus on the backs of the veterans that are out there.

MR. AUMENT. There have been -- I would acknowledge that too. I believe -- I feel that all of us in VA are very concerned about that, that we believe that we need to be doing more to try, as you have suggested, proactively to help assist veterans in this process.

Some of the solutions that I have seen proposed so far -- I believe that we will be seeing further steps that are going to be taken, but there has to have been some actual vetting of what the best solution actually is.

MR. MILLER. Do you know how long it takes to steal somebody's identity? We are vetting. We are how many weeks past the time it was stolen and we are still vetting?

MR. AUMENT. Part of the question there, Mr. Chairman, is whether or not all veterans want to have a solution imposed upon them, and that is -- one of the questions that we are wrestling with is, will all veterans, for example, want to have credit freezes or fraud alerts established on their accounts? Because there is some difference of views on that.

MR. MILLER. That is why I asked not about a credit freeze but a fraud alert. There is a difference.

Dr. Boozman.

MR. BOOZMAN. I will go ahead and yield again to the gentlelady.

MS. BERKLEY. Thank you, Chairman Miller and Mr. Boozman.

You said that you would like us to go to electronic as fast as possible. Is it a matter of money? Is it a matter of personnel? Because if I am here 20 years from now I have this sinking sensation that you and I will be having the same conversation.

One thing I have noticed about government is that we are very slow

to embrace technology. Even the United States Congress isn't where it needs to be.

Is it a matter of money or personnel or a lack of desire? When are we moving actually to the 21st century?

MR. AUMENT. Congresswoman, I believe it is probably a combination of all of the above to one degree or another.

There is probably -- one other factor to add to the list that you have just put out too is trying maintain our focus on bringing through to completion some of the projects that we are already undertaking -- VETS NET, for example. I am sure everybody wants to have an opportunity to mention that.

MS. BERKLEY. What is the current status of VETS NET, since I can only ask one question?

MR. AUMENT. We were up here on May 12th briefing the staff. We gave a relatively complete briefing there.

We are in the process of attempting to implement all of the recommendations that the Software Engineering Institute had given to us in their report they completed last fall, and we owe the committee a report back by the end of August with an end-to-end plan for implementation of VETS NET.

However, my point was that moving now to tackle an electronic records project, as valuable as it is -- I think that one of the reasons we are still uncompleted on VETS NET is moving to other distractions. And not that it is not a very important undertaking on that, too, but we believe that we need to first deliver on those things that we already have in progress.

MR. MILLER. Dr. Boozman.

MS. BERKLEY. Thank you.

MR. BOOZMAN. When will VBA be fully compliant with the Federal Information Security Management Act?

MR. AUMENT. The first steps we have at the moment are to complete the certification and accreditation, remediation projects that are on our plate. We have -- most of those are either under way or scheduled for completion. We believe that we should complete those. I would say that we could probably complete those within the next 2 years.

Some of those involve minor construction types of projects to control physical security, but I would say probably within 2 years.

MR. BOOZMAN. So compliant within 2 years, you think?

MR. AUMENT. I believe so.

MR. BOOZMAN. I guess, and I am trying to adhere to the chairman's wish of one question thing, but I would like to comment again, you have done a tremendous job of getting records. You are moving that right in that direction.

I am an optometrist. I know how it is with charts, when you have got 100,000 patients among the clinic and you have got a chart on somebody's desk. And you have a system of dealing with that now

that I am sure works pretty well. You lose charts now, you lose records.

On the other hand, we are faced with this challenge of moving over in the other direction. But it does seem like it makes sense to me that rather than the VA spending a tremendous amount of money, which we are doing -- Social Security spending a tremendous amount of money, DOD, Medicare. Medicare is pushing very hard for physicians to get all of their stuff electronic. So you can imagine the challenge that they are going to have in securing this stuff.

It does seem like the Secretary, yourself, your counterparts at HHS would sit down and say, I will give so much, you give so much, let's come up with a deal because it is interoperable as far as security. That is the only comment I have got.

I wish you would carry that back. And, again, somebody has got to show some leadership in this area and kind of get it going in the right direction.

MR. AUMENT. I will take that back, Mr. Chairman.

MR. MILLER. Ms. Herseth.

MS. HERSETH. Thank you.

On page 13 of your written testimony -- and you referred to it in your oral testimony today -- you mentioned that VBA is also considering expanding the use of terminal servers as a means of reducing or eliminating the amount of information stored locally on a remote user's work station.

I would contend that you need to move beyond considering and actually move to expanding it. And in the first hearing we had I shared a little bit of experience in the private sector where even at my work station in the office I couldn't save anything other than what was centrally located in the system, let alone accessing information remotely and storing it -- the way I read that is, if you are a remote user, that means you are outside of the VA facility, your office, and you are able to store something locally. That means at home, to me. That is sort of what brought us here today.

So I would just make that point and ask you if -- what are the barriers to expanding the use of these terminal servers? Is it just a matter of resources?

MR. AUMENT. Resources is a consideration, but it also takes some technical engineering as well to make sure that we would be able to put in place a solution such as terminal servers.

Let me suggest to you that we are already -- before we would even consider putting the ratings specialist back in a position working at home, that is, a solution that we would be imposing on them for any of the work-at-homes, would be that they would only be able to access the application, the RBA 2000, only be able to access that via terminal server.

Mr. Miller. Ms. Hooley.

Ms. Hooley. Thank you.

I am just going to go back to the fraud alert, credit freeze, credit monitoring.

Fraud alert and credit freeze are very different. Everybody can do a fraud alert that has had their data security breached. Not every State allows a credit freeze, we don't have a national standard, but you can do a fraud alert; and you need to tell veterans they can do that and what it means.

They can get a free credit report, which they need to do; and again, you can tell them all they need to do is call one number or go online and they can do that. So you need to make sure that they know that.

And then what I would hope you would do is look at -- for those that want it, that you have some kind of credit monitoring service, which I think is really how you best help the veteran.

I know, Mr. Miller, when you were talking about the veteran has to do this, the veteran has to do that, putting -- first of all, they need to know that they can do a fraud alert, a free credit report, but free credit monitoring is a one thing you can do for veterans. They still have to sign up for it.

I know I was a victim of a security breach, and they allowed us to have free credit monitoring; and actually what I was told is, they couldn't sign us up for it, but we could subscribe to it. So we got the paperwork at home; it was very simple, it was literally signing your name and a date, saying, I want free credit monitoring service.

I would hope that you would seriously look at that as an option for our veterans. I think they need some peace of mind, and that is really how they are going to get it, is through a credit monitoring system.

The question I have is, you talked about the number of files that are sitting in your -- one of your offices. How long is that going to take to get all of those on electronic files so that we don't have -- so we aren't losing, literally, documents that are -- I mean, they are not duplicated anywhere. How long is that going to take?

Mr. Aument. For the 20 million records that reside at our Records Management Center, Congresswoman, I would probably propose that we would probably never image those. Many of those are inactive files, some pertaining to deceased veterans that because of Federal records management requirements we need to maintain for some specified period of time. Many of those inactive files would not be certainly where we would begin in moving towards imaging of records.

We would likely begin probably making some conscious business decisions with those records that enter into the system that are newly created and entering into the system and going backwards then with those at the time that veterans reopen claims, possibly seeking increased ratings or claiming other disabilities.

We would probably try to put together a logical progression such

as that.

MS. HOOLEY. How long would that take?

MR. AUMENT. I have no idea.

MR. MILLER. Thank you very much for your testimony this morning. I am sure members have other questions and they will be getting to you after the hearing. Thank you very much.

I would like to ask the second panel, if they would, to move forward. While everybody's getting situated I am going to go ahead and introduce the second panel.

Mr. Michael Staley is the Assistant Inspector General for Audit at VA's Office of Inspector General. He is accompanied by Mr. Stephen Gaskell, Director of Central Office Audit Operations.

Mr. Gregory Wilshusen is the Director of Information Security Issues at the U.S. Government Accountability Office, and he is accompanied by Ms. Linda Koontz, Director of Information Management Issues.

STATEMENTS OF MICHAEL L. STALEY, ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY STEPHEN GASKELL, DIRECTOR, CENTRAL OFFICE AUDIT OPERATIONS DIVISION, OFFICE OF INSPECTOR GENERAL; AND GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, ACCOMPANIED BY LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

MR. MILLER. We thank you for being with the Subcommittees today; and, Mr. Staley, we will begin with you, please.

STATEMENT OF MICHAEL STALEY

MR. STALEY. Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify today on the results of our, reviews, which continue to address information security vulnerabilities in the VA and to report on the status of VA's implementation of our records.

I have with me today Stephen Gaskell, who served as a project manager on these IT audits.

We have conducted a number of audits and evaluations on information management security and information technology systems that have shown the need for continued improvements in addressing security vulnerabilities in VA and, as such, we have included IT security as a major management challenge for the Department in all of the major challenge reports issued since the fiscal year 2000.

In our annual financial statements we have reported VA information security controls as a material weakness since our fiscal year 1997 audit. Specifically, we have reported that VA's financial data and sensitive veteran medical and disability information are at risk due to vulnerabilities related to access controls, change controls, the need to segregate duties and the need to improve service continuity practices.

My IT security program auditors have identified and reported on significant information security weaknesses since 2001. All four of these annual audits have reported on similar issues, and the recurring themes in these reports are the need for a centralized approach and to achieve standardization, remediation of identified weaknesses, and accountability in VA information security.

For the Veterans Benefit Administration we have continued to report control weaknesses in access controls, physical security, electronic security and employee security. Our combined assessment program reviews continue to report security and access control vulnerabilities at VA regional offices where security issues were evaluated.

For example, at regional offices we have identified the need to strengthen physical security and access controls, procedures for providing employee security training and for obtaining background checks.

We have issued our most recent IT security program review in draft to VA for comment. While it is not our general practice to comment on draft reports before they are published, because of the extensive public interest in these information security issues, I have described the issues that VA is addressing in my written testimony.

In closing, I would like the committee to know the reviews of the VA's information security will remain a top priority for my office. We remain committed to reporting on the adequacy of IT security controls, and following up on actions taken by VA to strengthen these controls, we remain dedicated to the goal of protecting our Nation's veterans.

Mr. Chairman and members of the subcommittee, thank you again for this opportunity. I would be pleased to answer any questions.

[The statement of Mr. Staley appears on p. 54]

MR. MILLER. In the past, the IG has found some instances where terminated or separated employees retained access to critical systems identified at various locations.

Whose responsibility is it to ensure that former VBA employees don't have access to computer systems and information and such?

MR. STALEY. That is correct, Mr. Chairman. We have been finding that during our combined assessment program reviews. Access con-

trols actually have been found during our financial statement audits and when we do testing during our FISMA reviews.

MR. MILLER. Can you tell who is making -- are they accessing or do they just have the ability to access?

MR. STALEY. They have the ability to access.

MR. MILLER. Are you finding that anybody is trying to access after the fact?

MR. STALEY. Not any specific examples I can give you at this time.

MR. MILLER. I would go to Dr. Boozman, but he will yield to Ms. Berkley. So Ms. Berkley.

MS. BERKLEY. Cut out the middleman.

Let me ask you a question. According to your opening statement, this was a disaster waiting to happen, so I assume that you weren't overwhelmingly surprised when this theft occurred?

MR. STALEY. I would have to say that I think you are always concerned when something like this happens to -- whether it be one veteran or all of us veterans. I know myself, my data is also on that listing.

MS. BERKLEY. My husband received his letter as well.

Had the VA implemented your recommendations, could this have been avoided?

MR. STALEY. It is very difficult to say whether this particular incident could be avoided. The issues that we have talked about for these many years have addressed network security issues, access control issues.

In response to this specific issue, we do have an administrative investigation ongoing which we hope to report on to the Department at the end of this month. And we will be asking for comments and hope to actually issue the report for you mid-July or so.

MS. BERKLEY. During the prior two hearings on this topic, we heard a significant amount about the culture at the VA. This culture is characterized as entrenched and indifferent relating to IT projects.

Does VBA's fielding of VETS NET, a project that is in the works for over a decade now, relate to such cultural problems?

MR. STALEY. I think what we had been talking about is the 16 or so issues that we presented, before you really speak to the issue of standardization; and that can only be accomplished if the three administrations work collectively to address them as one voice.

MS. BERKLEY. Is VETS NET the solution to the problems?

MR. STALEY. Well, VETS NET is a solution to an aging benefits delivery network system. I think -- of course, I joined the VA in 1971, and I believe Target 1 by Honeywell was just starting at that time, so it is 30 years, may even be 40 years old. We need to find solutions to replace these platforms, and VETS NET is attempting to do that.

We have not reviewed VETS NET, we have not studied VETS NET; we are waiting for this contractor to complete his review, which I be-

lieve is due this summer. But we have been overseeing the progress and getting briefings on the progress of VETS NET.

Ms. Berkley. Thank you.

Mr. Miller. Dr. Boozman.

Mr. Boozman. Thank you, Mr. Chairman.

Earlier we had testimony that VBA estimates that they will have full compliance in 2 years with the Federal Information Securtiy Management Act. Do you feel like that is possible?

Mr. Staley. I feel for many of the issues that we have been identifying each year, the fixes are fairly dependent on vigilance. It is an issue of having very strong access controls, having your users only have information that they need information for. Many of these fixes can be done relatively soon.

For the bigger issues, such as VETS NET and replacing platforms, I do know that the Department is working on these major system initiatives; and I have seen their timelines and charts and whatnot. Some of them are out to fiscal year 2008, 2009 and 2010.

Mr. Boozman. As we move -- is that a "yes" or a "no"?

Mr. Staley. For many of them, a 2-year timeline is feasible. For platform replacement issues, I could not say.

Mr. Boozman. When you get into going from one extreme to the other, when you get into encrypting and things like that, will that slow down -- do you run into problems then with a slowdown of the systems?

Mr. Staley. That is one of the issues that the Department is facing with many of these aging systems and that they were constructed 30-some-odd years ago. From what the technicians are telling us, that could be a possible outcome to adding software that would encrypt data. So it is possible.

Mr. Boozman. Our current system, can it identify instances of large downloads of data?

Mr. Staley. It is my understanding that you can -- you will get a log of the time that someone is in a system but not necessarily what is being downloaded.

Mr. Boozman. Do you, in investigating this and being a part of it, do you see any accompanying legislation that we need to do for VA to help them in dealing with the problem?

Mr. Staley. Well, I am really not in a position to comment on new legislation. Obviously, from my audit perspective, compliance with FISMA and remediating the issues that we have identified is one issue. I do know thatsometime in May, OMB issued instructions to all the agencies to take a strong look at the security issue, which I believe they are required to report in their next FISMA report in 2006.

Mr. Boozman. You mentioned security access and then also you mentioned background checks. So we have got the problem that we are dealing with in this regard, and then too, as far as the back-

ground checks, to actually -- even if you have those systems in place and having the appropriate people hired, what is the problem with background checks?

We learned at an earlier hearing that we have a physician that has a history of being a sexual offender. What's the deal?

MR. STALEY. From what we are seeing, it is a coordination problem from the point of the program office that that employee begins to work for, the HR division that is responsible for processing paperwork, and then the security and law enforcement. So it is the process of actually requesting these background checks timely, to get them done.

And then the Department has also discussed the fact that it does take time to do these background checks; but there are various tiers of background checks that can be performed, and some of them only require law enforcement, fingerprinting-type procedures, and others are far more extensive and they take more time.

MR. BOOZMAN. Does it is make sense that all of our agencies -- again, Medicare, as they go to an all-physician record situation and stuff where all that is digitalized and things, does it make sense for the agencies to talk to each other and try and figure this out together versus spending millions of dollars independently?

MR. STALEY. It would make sense to communicate and work with as many agencies as possible.

MR. BOOZMAN. Thank you, Mr. Chairman.

MR. MILLER. If we could, Mr. Wilshusen, if you would proceed with your testimony.

STATEMENT OF GREGORY WILSHUSEN

MR. WILSHUSEN. Chairman Miller, Chairman Boozman and members of the subcommittees, thank you for inviting us to participate in today's joint hearing on data security at the Veterans Benefits Administration.

The recent well-publicized security breach at the Department of Veterans' Affairs has highlighted the importance of good information security controls and protecting personally identifiable information not only at VA but throughout government.

As we have reported on many occasions, poor information security controls is a widespread problem that can have devastating consequences such as the disruption of critical operations and unauthorized disclosure of highly sensitive information.

Today, I will discuss the recurring security weaknesses that have been reported at VA, including those at VBA, what agencies can do to prevent breaches of personal information and the notification of individuals when such breaches occur.

Since 1998, GAO and the VA IG have reported on wide-ranging deficiencies in VA's information security controls, including the lack

of effective controls to prevent individuals from gaining unauthorized access to VA systems and sensitive data. In addition, the Department had not consistently provided adequate physical security for its computer facilities, assigned duties in a manner that segregated incompatible functions, controlled changes to its operating systems, or updated and tested its disaster recovery plans.

These deficiencies existed in part because VA had not fully implemented key components of a comprehensive information security program, including the lack of centralized management and an approach for addressing security challenges.

Although VA has taken steps to improve security, its efforts have not been sufficient to effectively protect its information and information systems. As a result, these remain vulnerable to inadvertent or deliberate misuse, loss or improper disclosure, as the recent breach demonstrates.

In addition to providing and implementing a robust security program, agencies such as VBA can better protect personally identifiable information by conducting privacy impact assessments that determine up front how personal information is to be collected, stored, shared and managed, so that controls can be built in from the beginning, by limiting access to the information and training personnel accordingly, and appropriately using technology controls such as encryption.

VBA officials have informed us that since the May 3rd incident they have taken, or plan to take, a number of steps to enhance protection of veterans' personal information. These include reviewing and recertifying user access to sensitive information, evaluating encryption technologies for transmitting and storing data, and requiring privacy and cybersecurity training for all VBA employees by June 30.

Although we have not reviewed these actions and cannot comment on their sufficiency or effectiveness at this time, they appear to be important first steps. However, the true test will be VBA's ability to fully implement and sustain appropriate protections over the long term.

Nonetheless, even with security and privacy protections in place, breaches can occur, particularly if enforcement is lax or employees willfully disregard policy. When such breaches occur, appropriate, sufficient, and timely notification to those affected have clear benefits, allowing people the opportunity to protect themselves from identity theft.

In summary, long-standing control weaknesses at VA have placed its information systems and information at increased risk of misuse and improper disclosure. Although VA has made progress in mitigating previously reported weaknesses, it has not taken all the steps necessary to address these serious issues. Only through strong leadership and sustained management commitment can VA implement

a comprehensive information security program that can effectively manage risk on an ongoing basis.

Mr. Chairman, this concludes my statement. Ms. Koontz and I will be happy to answer questions.

[The joint statement of Mr. Wilshusen and Ms. Koontz appears on p. 64]

Mr. Miller. In terms of information security can you give us some type of a feel as to how VA or VBA fits within other agencies? Is everybody failing?

Mr. Wilshusen. No, everybody is not failing. One measure that would be important is, the FISMA reports that agencies are required to submit to Congress and to the OMB regarding their implementation of the provisions of the Federal Information Security Management Act, or FISMA. Each year we perform an analysis of those reports, and we found that over the past 4 out of 5 years VA typically has ended up towards the bottom end of the scale whereas other agencies, particularly some of the smaller, single-mission-type organizations tend to score higher. But what VA has done, too, is not dissimilar to other large complex organizations.

Mr. Miller. Do you have any role in seeing that your recommendations are implemented? Is there any follow-up at all with the reports that you make?

Mr. Wilshusen. Yes, there is. We follow up on all of our recommendations that we make, yes.

Mr. Miller. And when a recommendation is not followed then next year, you bring it up again and you follow it up and you do it again next year? It would seem pretty exasperating if that was what your job was year in and year out.

Mr. Wilshusen. We do find that agencies, including VA, do take some corrective actions to address specific weaknesses, but often they do not address the larger recommendations that relate to the underlying causes of those weaknesses.

For example, we have routinely reported -- again, we haven't done much work at VA for a number of years, but we would follow up and look at the underlying reasons that we felt dealt with not having a comprehensive information security program that has been fully developed, documented and implemented at the agency.

And so what that does is, while they may take corrective actions on specific technical findings that we identify, often what may happen is, they only correct them at the sites or the systems that we looked at and they don't look across the organization, across other similar systems, to take corrective actions on those same weaknesses.

Mr. Miller. Do they ever come back and say, this is a distraction, we can't deal with this right now, we have this other thing we are working on right here?

MR. WILSHUSEN. Never in those blunt words. We often -- often they concur with our recommendations, and I think they try to take action. But sometimes it is a challenging endeavor for many organizations in the Federal Government because, one, the computing environment is very complex and the threats and the types of risks are constantly changing. It is a very dynamic environment.

There are challenges. But with appropriate and well-defined and executed information security programs, they can address those risks.

MR. MILLER. Thank you.

MS. BERKLEY.

MS. BERKLEY. Thank you. I wish that we would have had this panel before the first panel because I would like to have heard the first panel's response to some of your testimony.

Since May 3rd, have you detected any change in behavior or attitude with the VA? In your opinion, do they recognize the seriousness of what has transpired and are moving to implement corrective action so this can't happen again?

MR. WILSHUSEN. We had one meeting with the VBA officials in order to collect some of the information about actions that they have taken or plan to take in response to this incident. Just from that one meeting it seems like they are very concerned and are trying to take the actions, but again, the proof is in the pudding.

Once the actions and policies have been decided and developed, they need to execute and implement those. That will take time and commitment over a long period of time.

MS. BERKLEY. So you had a meeting with the VBA officials, discussed with them what they need to do. And now how do you follow up and make sure this is happening? Or is that not your job? If it is not your job, whose job is it?

MR. WILSHUSEN. Actually, the work we do is, by and large, requested by -- either requested by Congress or congressional committees and/or mandated.

We have received several requests, and there have been some potential mandates proposed where we would do some work in this area, but we have not done any yet.

MS. BERKLEY. Perhaps Mr. Boozman is going to ask the question that he asked previously, but what is it that -- would you need any additional legislation from Congress, or how could we do our jobs better so that you can do your job better, and ultimately, VBA and the Veterans Administration can protect the privacy of our veterans?

MR. WILSHUSEN. Well, with regard to information security, as Mr. Staley pointed out, there is a law called the Federal Information Security Management Act of 2002, FISMA, and that provides a comprehensive framework for implementing security throughout a Federal agency; assigns specific responsibilities to the head of the agency,

senior managers, to the CIO. In addition, it requires each agency to develop, document and implement an agency-wide security information program that contains several elements.

That law has, I believe, raised the level of attention given to information security and provides a solid framework for agencies to follow in order to implement better security.

The fact is that many agencies still have difficulty in fully implementing those programs. So I don't know if additional legislation is needed. Certainly in terms of what we need to do in having been requested to go in and do follow-up work, we can do that.

MS. BERKLEY. Thank you.

MR. MILLER. Dr. Boozman.

MR. BOOZMAN. Thank you.

Mr. Wilshusen, we talked earlier about H.R. 4061, and the approach the committee felt might be a little more effective by centralizing the system a little bit more than they are now. As you work with the other agencies, can you comment on that? Is this something that you found to be effective or is the decentralized approach better?

MR. WILSHUSEN. We haven't done a systematic review of the other Federal agencies in terms of their organization, of how the CIO is organized relative to the other program offices; but what we have found is that for information security, centralization having a central management approach is preferable, because the interconnections between the systems and the types of policies and procedures that are in place at one agency or component could have an impact on other elements or components within that agency.

So we wholeheartedly endorse having a centralized managed approach to implementing security at a Federal agency.

MR. BOOZMAN. As you deal with these problems system-wide, it does seem like -- again, with Medicare pushing hard to get electronic records, things like that, that ability is far outpacing again the transition from where do we put the charts, where do we put the records versus we can secure that, how do we secure this other thing.

What -- in your experience, what agencies are doing a better job?

MR. WILSHUSEN. Well, certainly the use of electronic records and using the interconnectivity of systems has brought tremendous benefits to Federal agencies in terms of being able to deliver government services to the people. But those same benefits and opportunities are subjected to and can create significant risks if adequate safeguards are not built into those technologies.

We have found that it is imperative that agencies consider and build security into these systems from the very beginning throughout the entire life cycle, rather than trying to add them on as an afterthought. They tend to be more expensive and they tend to be less effective.

So certainly one of the things that agencies need to do when con-

verting paper records to electronic records is think about and implement and design security controls up front.

MR. BOOZMAN. Is there a model agency out there?

MR. WILSHUSEN. I think that probably some of the different agencies have varied experiences in doing this. I don't know if there is a model agency per se in terms of implementing security on electronic systems. At most of the agencies we go to, where we have done specific testing of the controls, we generally find weaknesses on each system or most of the systems we look at.

MR. BOOZMAN. It doesn't make sense -- again, I am harping on this. It doesn't make sense to me; I guess I am asking if it does to you.

But we want VA -- and VA has done a good job of switching over; we want VA to be able to talk to DOD. We want Medicare -- I think we will foresee a time where Medicare and VA should be talking to each other as far as medical records and pharmacy records and all those kinds of things.

But it does seem like, in making things interoperable and in solving some of these problems, you want more access to the records through all these different agencies. But then how do you secure that access?

It does seem like that needs to be set up as you go along, as you just said, rather than trying to backtrack at some point and figure out how do we do this.

I guess my question is, how do you do that? There doesn't seem to be much talk among the agencies, so that -- you really wouldn't comment on a model out there, but I am sure there are some good ones that are better than others.

How do we get that done?

MR. WILSHUSEN. Well, one way is, what agencies need to do -- and I believe there is a CIO Council that can meet to discuss issues that cut across different agencies. And certainly this could be a topic for that council to start addressing, looking at government-wide security requirements that are needed for these systems as they develop them. So that would be one way, through there.

But definitely what agencies need to do, as they develop their systems, is to assess the risks, categorize the type of information they are going to be collecting and storing on those systems, and determine what the appropriate level of security over that information will be.

MS. KOONTZ. If I can just add, from a privacy perspective, too, this is one of the reasons that we have emphasized the importance of agencies implementing the privacy impact assessments which are required under the
E-Government Act, and that is a way of looking at the implications of collecting, handling and disseminating personally identifiable information in an agency and being able to build controls up front before the information is collected and before the system is built.

You are absolutely right that once these things are done, it is very difficult to retrofit. And I think that you are also right in that technology is creating tremendous challenges for agencies in terms of balancing accessibility with security and privacy concerns; and I think there is a role here for the Congress in terms of policy, as well as for agencies in terms of implementation.

MR. BOOZMAN. Thank you very much.

Thank you, Mr. Chairman.

MR. MILLER. Dr. Boozman, any closing comments?

MR. BOOZMAN. I appreciate your leadership in this area and getting the two committees together. I think the VA is to be complimented in the sense that it has done a very good job of moving forward. We pressed them hard to get the records in digital format and things like that.

So we have done a good job that way, but we have lagged much, much behind and as we have talked about, having the security that goes along with that. It is something that not only VA has got to work very hard on, but it is a system-wide problem. Testimony mentioned the problems not only of the data but having the right people there.

So there are so many things like this that we have really got to shore up not only in the VA, but system-wide.

Again, I know that our Subcommittee, the Committee in general, in a very bipartisan way, is committed to doing whatever it takes legislatively to give the agencies, in our case, specifically, the VA, the tools.

Thank you, Mr. Chairman.

MR. MILLER. Thank you very much, also, for your leadership and again for a bipartisan approach.

We thank everybody for their testimony today. While there has apparently been no identity theft that we are aware of, we all agree that the potential is great. We must continue to work together to make sure that nothing like this happens again, and while this information continues to be floating out there somewhere, that nobody's credit or identity is harmed by what has happened.

I appreciate everybody being here today. Members will have 5 legislative days in which to add their statements to the record.

[The statement of Mr. Udall appear on p. 39]

Mr. Miller. Without any further comment, this joint subcommittee meeting is adjourned.

[Whereupon, at 11:54 a.m., the joint hearing of the subcommittees was adjourned.]

APPENDIX

Congressman Tom Udall (NM-3)
House Veterans Affairs Subcommittee on Disability Assistance and Memorial Affairs
Joint Hearing on VBA Data Security
June 20, 2006

Mr. Chairman,

Last month, we learned that the information of 26.5 million veterans and 2.2 million active duty and reserve service members was compromised. The opportunity for this to ever happen again must be eliminated. I hope that today's hearing will give the VBA, and by extension the VA, the chance to sincerely and thoroughly review its IT security efforts and construct comprehensive security procedure that will properly secure the personal information of every single veteran. We must make every assurance to veterans that we are taking the necessary steps to improve what is obviously a broken system.

For six straight years, the Office of Inspector General (OIG) has released annual reports which characterize VA IT security with terms such as "weaknesses," "vulnerabilities," and "failures." In every one of those years, the OIG identified the area of IT security as a "major management challenge." And in today's testimony from Mr. Staley, it is noted that not only have the sixteen issues of concern from last year's OIG report not been addressed, a new issue has been added. This is simply unacceptable.

I hope to hear from the VBA officials here today what process is underway to address the OIG concerns, and to do so in the most effective, efficient, and swift manner as is possible. As a side note, I do regret that the VBA testimony was not available until just this morning, as it did not allow proper time for review by committee members.

Millions of veterans are now wary of the VA because of last month's data loss. Not only is it the job of the VA to change its security process and to change the procedure used to deal with such situations, but it must also convince veterans that it is to be trusted. The VBA is one of the most vital components of starting down that path, and it must put forth every effort to perfect its systems and to better serve all veterans at every step.

Thank you, Mr. Chairman.

Statement of Ronald R. Aument
Deputy Under Secretary for Benefits
Before the
Subcommittee on Disability Assistance
and Memorial Affairs
and the
Subcommittee on Economic Opportunity
June 20, 2006

Chairman Miller, Chairman Boozman, and Members of the Subcommittees, thank you for the opportunity to appear before you today to discuss data security in the Veterans Benefits Administration (VBA). I am accompanied by Mr. Jack McCoy, Associate Deputy Under Secretary for Policy and Program Management, Mr. Michael Walcoff, Deputy Under Secretary for Field Operations, and Mr. Thomas Lloyd, Deputy Chief Information Officer in VBA.

Let me assure the Subcommittees that VBA is thoroughly examining every aspect of our information security program, our processes, and our procedures to ensure that sensitive veterans' data is neither mismanaged nor used for any unauthorized purpose. Although our review is ongoing, I will outline those security measures in place prior to May 3, 2006, what we have done to communicate with veterans about the data theft, and additional steps we have taken regarding our data security policies and procedures. I will also specifically address the security of the data feeds between VBA and DoD.

We take the privilege of serving veterans very seriously, and we have taken direct and immediate action to address and alleviate veterans' concerns and to restore their confidence.

IT SECURITY POLICIES AND INITIATIVES PRIOR TO MAY 3, 2006

VBA has incorporated security into its information systems and processes to support the delivery of veterans benefits. VBA has extensive, well-articulated policies and procedures governing information access requests, auditing, and rules of behavior. These policies and procedures pertain to all VBA employees, as well as to those individuals, including consultants, to whom VBA authorizes access to VBA systems and data.

Responsibility for all IT security policy is centralized to the Department's Office of Cyber and Information Security, which reports directly to VA's Chief Information Officer. Implementation of IT security policy and procedures in VBA is through a three-layer organizational assignment of responsibilities. The Information Security Officer (ISO) at each regional office is responsible for the execution and oversight of IT security policy and procedures. The Network Support Centers (NSCs) provide oversight of regional office (RO) compliance with IT security policy and procedures and expert advice to the RO ISO community and IT staffs on technical issues. The VBA IT organization in Headquarters provides the technological support that implements IT security and procedures on the computer applications and systems managed for VBA.

All 58 VBA ISOs nationwide, as well as the employees of the Network Support Centers and VBA Headquarters security staff, were detailed to the VA Office of Information and Technology on May 1, 2006, as part of the implementation of the VA IT Federated Model. They will be permanently assigned to that office on October 1, 2006.

VBA centrally controls the standard configuration of servers and VBA desktop and laptop computers. We deploy updates automatically to maintain quality assurance and security. When a server or workstation is connected to the network, the VBA standard configuration is automatically loaded.

VBA also has a secure technology solution in place for individuals requiring access to our systems from outside our controlled LAN environment. That solution requires external users to access VBA systems through the One-VA Virtual Private Network (VPN) to a Centralized Terminal Server. The One-VA Virtual Private Network (VPN) allows remote users to access VA systems in a secure environment. In addition, the computers used for VPN access must be protected through the use of the Office of Cyber and Information Security approved anti-virus and "personal firewall" software prior to using VPN. The use of this software is required for VPN access to protect the VA network from communications containing potentially malicious software. VPN data communications are encrypted.

The One VA Terminal Server, located in the VBA-controlled computer room, contains all the files, programs, and database information. VBA outbased workers, as well as authorized Veterans Service Organization (VSO) representatives, use this capability. Additionally, the Veterans Information Portal provides secure, encrypted user access to Loan Guaranty applications for internal and external users.

VBA has established rules-of-behavior policies that comply with VA requirements and govern the use of IT systems and capabilities maintained by or for VA. All users authorized to access VA systems through Local Area Networks or through the One VA Virtual Private Network are required to sign VBA-specific rules of behavior. VBA rules of behavior have also been developed for employees authorized to use government-owned laptop computers. These VBA rules of behavior ensure all users of VA IT resources are aware that any system potentially contains valuable and sometimes sensitive government and/or personal information, which must be protected to prevent disclosure, unauthorized changes, and loss.

Individuals are granted systems access by delegated approving officials who determine access levels based on the employees' work requirements. Prior to being given access permissions, each individual requesting access to a VBA information system must sign a certification of receipt and understanding of the VBA-specific rules of behavior governing the use of VBA IT resources. The rules of behavior advise users that misuse of government systems, mishandling of veteran data, or unauthorized disclosure of sensitive information could result in disciplinary action up to and including termination of employment. During regular site visits, VBA's Network Support Centers review user security folders maintained by the ISOs to ensure signed rules of behavior are in the folders.

User password construction requirements and expiration limits for all VBA applications comply with VA requirements. Additionally, users must complete both security and privacy training. The Secretary recently directed that all employees sign a Statement of Commitment and Understanding on completion of the training, confirming their understanding of the training, their commitment to protecting sensitive and confidential information, and the consequences for noncompliance.

VBA also has a formal process for requesting data extracts from VBA information systems. A Project Initiation Request (PIR) is a request to the VBA Office of Information Management (OIM) for information technology services initiated by both VBA and VA entities. The PIR is prepared primarily by a sponsor organization to notify OIM of a new system requirement, a modification or change to a requirement, an enhancement to an existing system, or a request for a data extract or match. For example, VBA provides 15 different extracts from the Beneficiary Identification and Records Locator System (BIRLS) to internal VA organizational elements as well as external agencies. Data is matched and/or extracted from BIRLS for purposes such as identification of inactive claims folders eligible for retirement to a storage facility; verification of veteran status for Department of Education benefit applicants; identification of VA

employees in the PAID system who are also veterans; death matches with the Veterans Health Administration and the Social Security Administration; investigations by the Office of the Inspector General; and research projects by the National Academy of Sciences Institute of Medicine. Additionally, there are four interfaces or data feeds into BIRLS: two from the Defense Manpower Data Center for new servicemembers and reservists and to provide retired pay information; one from the VBA Benefits Delivery Network (BDN) claims processing system to update BIRLS based on recent BDN record changes and transactions; and one from the Veterans Assistance Discharge System (VADS) for recent separatees. Each extract and interface was established through a formal VBA approval process. Modification of any data provided electronically is prohibited.

In 2005, VBA issued a detailed directive for Information Security Officers (ISOs), who are critically important to data security. ISOs manage local access control to IT resources, conduct security audits, and are the focal point for incident reporting in a VBA facility. The VBA internal controls process requires local systematic analyses of operations. RO directors certify annually that their facilities are in compliance with VBA directives.

VBA Network Support Centers also conduct annual surveys of IT operations and security controls, policies, and procedures at their client ROs within their geographical area of jurisdiction. The primary purpose of these on-site security visits is to ensure that the ROs are adhering to all VA, VBA, and other federal security directives and handbooks and that deficiencies identified in previous CAP reviews are remediated.

VBA completed the Federally mandated certification and accreditation (C&A) of 97 application systems on schedule in August 2005. We will maintain C&A through a 3-year C&A update cycle.

The VA Office of Inspector General (OIG) regularly conducts independent examinations of VBA operations. For example, through the Combined Assessment Program (CAP), OIG examines all RO business processes, including adherence to information security policies and directives. We have reviewed all IT and security-related findings and recommendations made during FY05 and FY06 OIG CAP Reviews. The majority of identified deficiencies are remediated during the time the OIG is still on site. Recommendations that cannot be remediated immediately are referred to the Network Support Center (NSCs) to ensure appropriate and timely remediation. Action has been completed on all recommendations made by the OIG during the CAP reviews, and all recommendations have been closed by the OIG.

The Department has improved controls through the establishment of the Office of Cyber and Information Security (OCIS); VBA continues to update and enhance internal policies and procedures. In 2002, VBA issued comprehensive directives for IT Systems General Security Requirements (April 2, 2002) and Benefits Delivery Network Privacy and Security (August 28, 2002). These policy directives were revised and updated January 6, 2004. On January 28, 2005 we distributed another handbook that provided all VBA Information Security Officers with detailed guidance regarding their duties and responsibilities for RO security operations.

As part of our ongoing efforts to strengthen IT security, VBA has successfully tested its disaster recovery procedures for 29 of 31 major applications, and has invested in a fully redundant system to provide disaster recovery for the Benefits Delivery Network (BDN). The system has been installed, and a test of the recovery of all BDN applications was completed in September 2005. The test will be repeated yearly.

VBA is in the process of completing the final two core applications of the VETSNET system, which will replace the legacy Benefits Delivery Network

system for delivery of compensation and pension benefits. VBA continues to build security and appropriate audit trail capability into VETSNET. VETSNET applications utilize journal tables in the corporate database to retain the sequence of events that change the records for each veteran and claimant record. Every corporate database table containing veteran and claimant data has an associated journal database table. Every VETSNET application transaction that changes veteran and claimant data is journaled. Journal information includes the state of the record prior to the change, the change made, the user enacting the change, the station from which this change occurred, and the date and time the change was entered.

Specific Business Line Access Issues

In all VBA's benefits systems, veteran data is protected by VBA security policy and IT system and application security controls. Programmatic access controls restrict access according to the specific veteran record level of sensitivity and the authority of the individual accessing the data.

Veterans Service Organization (VSO) Access to Veterans' Information

VSOs are strong partners in VA's mission, providing advice and representation to millions of veterans and their dependents each year. The law permits VA to disclose information on specific VA claimants to "duly authorized" VSOs. In performing their duties, the VSOs routinely access sensitive VA information regarding their clients. Claimants or beneficiaries must sign a power of attorney to allow a VSO to obtain access to their records.

VSO representatives who are co-located at VBA sites, as well as many VSO representatives who work at non-VA facilities, have access to some of the same IT systems which VA employees access. These systems are restricted so that VSO representatives can only access information regarding their organization's clients, and only if they have a power of attorney. In addition to VA's procedures for safeguarding sensitive information, the Veterans Service

Organizations themselves have procedures for controlling access and dissemination of such information. The One-VA Virtual Private Network (VPN) allows remote VSO users to access VA systems in a secure environment.

Outbased Employees

VBA has a significant number of employees who are required to be out-based by the nature of their positions and who must have personally identifying information for VA beneficiaries available to them in order to carry out their responsibilities. Employees working in the field and at outbased locations are needed in almost all of VBA's business lines.

Field examiners make periodic home visits to VA beneficiaries and their fiduciaries to assess their competence, adjustment, and personal welfare. Education Compliance Survey Specialists and Education Liaison Representatives travel to schools to review student records. VR&E Counselors are located in more than 120 outbased locations, providing improved access to veterans in communities distant from our regional offices. Loan Guaranty's Monitoring Unit performs oversight of VA lender operations through a program of performance audits conducted on site at lenders' offices and at their home office in Nashville. We ensure that our outbased offices have the same level of security that our Local Area Network (LAN) environment offers in VA facilities. Employees such as Field Examiners who often work out of their homes access VA systems through the One VA VPN.

QTC Medical Examinations

Since 1998, VBA has contracted with a private vendor, QTC Medical Services, Inc., to perform approximately 16% of our disability examination workload. This program was initiated under the authority of P.L. 104-275 and has become a standard program since that time to supplement the need for disability examinations at ten regional offices.

The data used by QTC for medical examinations is entered into the Veterans Examination Request Information System (VERIS), maintained on VBA's Intranet server by Veterans Service Representatives at the ten regional offices and their Benefits Delivery at Discharge (BDD) sites. Each night, the VERIS server compiles an encrypted file that is transferred to QTC for downloading into QTC's password-protected internal network.

For claims that require the examiner to review medical documentation, the regional offices ship the claims folders by FedEx. QTC scans and prints the medical documentation and sends the information to the examiner using USPS overnight priority mail. When the examiner has completed the examination, the documentation is shredded. QTC is responsible for returning the claims folders within five days of the completed appointment and uses UPS ground services for shipping.

The contract requires that QTC post the completed examination reports on a secure website and only provide access to VBA-authorized users. QTC employees e-mail VA employees through the use of VPN and have access only to VBA's Exchange e-mail server.

Vocational Rehabilitation and Employment Contract Counselors

The Vocational Rehabilitation and Employment program utilizes contract counselors to supplement and complement the work performed by VA counselors. These contract counselors do not have access to VBA computer

systems or any VR&E computer applications. Contract counselors are provided with paper copies of veterans' VR&E records from the Counseling/Evaluation/ Rehabilitation (CER) files. These records do contain veterans' personal information. Contract agreements contain specific clauses regarding privacy and security, in which the contractor commits to secure all information. In addition, many of the contract counselors are Certified Rehabilitation Counselors and are held to the Code of Professional Ethics from the Commission on Rehabilitation Counselor Certification, which directly addresses the confidentiality of client records. VR&E Officers are responsible for ongoing audits of contractor work.

Loan Guaranty Contractors

Electronic data transmissions between Loan Guaranty Service and its contractors, Ocwen and Countrywide Home Loans (CHL), are via a secure communications network. Both Ocwen and CHL have documented and tested procedures and policies regarding control and release of information. These range from restricted access to the use of internal audit and oversight groups who monitor compliance. There are also external audits conducted to monitor compliance. Both contracts include specific requirements that charge the contractor with data and system security. VA audits these contractors, as do auditors both internal and external to the companies.

ACTIONS TAKEN TO INFORM VETERANS ABOUT THE DATA THEFT

VA has taken aggressive action to notify veterans and to respond to their inquiries regarding the data theft. Upon learning of the data theft, VBA developed a plan for staffing and training regional office public contact teams, working extended hours, and enhancing our telephone system capacity. We contracted with the General Services Administration to provide commercial call center services to answer veterans' calls about the loss of personally identifiable information. VBA staff met with contractors to set expectations and to review procedures. A VBA employee is on site at each contracted call center location to provide assistance and guidance. Scripted responses to potential questions

were developed for the call centers and regional office public contact staff. These scripted questions and answers have been updated as we learn more about the situation and gain experience with the nature of the concerns expressed by the callers.

Since our veterans are increasingly using the web and e-mail, we established a single center to respond to these queries and to ensure uniform, correct information is delivered.

We also updated and strengthened procedures for handling veterans' requests to change address and direct deposit information to ensure proper verification of identity of the individual requesting the change. In an average month, we receive in excess of 40,000 requests from VA beneficiaries to change their financial institution and/or address.

TECHNICAL AND POLICY CHANGES SINCE DATA LOSS INCIDENT

In March of this year, just prior to the data theft incident, we started the process to accelerate implementation of Public Key Infrastructure technology (PKI) throughout VBA. PKI will provide a common utility for VA to support more secure electronic transactions and e-mail. It will allow VBA users to more securely send veteran-sensitive information (social security number, medical conditions and diagnostic codes, etc.) to VHA and other VA elements.

Since the May 3 security incident, VBA has supported the Secretary's direction to accelerate the annually required Privacy Awareness and Cyber Security training. VBA's previously issued training directives required training to be completed by the end of the fiscal year. All VBA employees are now required to complete these training programs by June 30, 2006.

VBA is also examining the data and systems used to test applications prior to deployment to ensure that any veteran data required for applications testing or data analysis is properly protected or scrambled to prevent disclosure.

We have compiled a list of all VBA databases that contain sensitive information and all interfaces or data feeds that update these databases. We have compiled reports from each program and staff office regarding what VBA data is released to other VA and external entities. We have compiled all documented policies and procedures that govern the release of this information. A VBA work group has been tasked with assessing all current VBA policies and procedures related to the release of data protected by the Privacy Act. The work group will then provide recommendations to improve protection of the data to include periodic recertification of the business need for the release.

Effective June 7, in accordance with the Secretary's direction, VBA suspended all work-at-home and flexiplace arrangements for employees directly involved in disability claims processing. Field station managers were ordered to immediately recall these work-at-home and flexiplace employees to VA offices and to ensure they returned all claims folders and computer equipment when they came back into the office. Those employees who adjudicated claims at their homes or other non-VA work sites will now do all claims work requiring claims files in regional offices. This suspension of work-at home and flexiplace arrangements involving claims adjudication will continue while VBA evaluates various solutions to protect sensitive data transported to and from offices, particularly by work-at-home and other flexiplace employees. We are reviewing existing policy, directives, and letters regarding work-at-home and flexiplace. We are also developing a standard work-at-home and flexiplace agreement to ensure all employees absolutely understand their responsibilities to safeguard sensitive data.

VBA has procured encryption capability for laptop computers. We are also considering expanding the use of "terminal servers" as a means of reducing or eliminating the amount of information stored locally on a remote user's workstation. Under the "terminal server" configuration, remote users are restricted to only displaying and updating documents on their computer screens. All of the users' data and documents are created and maintained on a terminal server at a VA facility. In conjunction with VA's Office of Cyber and Information Security, we are also participating in the evaluation of a centrally managed encryption solution for computers and removable devices.

VBA Information Security Officers are required to review all users' access and privileges at least quarterly, or when a job change occurs that may require a different level of access with local business managers. Accounts on all systems are disabled after 90 days of inactivity and deleted after 180 days of inactivity. As a result of the data breach, the Secretary tasked all administrations to inventory current users of their information systems and provide a single database that contains these records. VBA is executing the Secretary's direction to centrally identify all individuals who have access to sensitive information.

We are also working with the Office of Acquisition and Materiel Management to reinforce strong control of the shipping of records containing personally identifiable information. This includes review of tracking procedures, signature requirements and expedited shipments.

DoD DATA FEEDS

Finally, let me address the issue of data feeds to and from VBA and the Department of Defense.

The VA/DoD Joint Executive Council (JEC) was established as a result of the President's Management Agenda. This council is charged with enhancing

coordination and resource sharing between VA and DoD and satisfying the reporting requirements of Public Law 97-174 and Public Law 108-136. VA and DoD together have made substantial progress toward data sharing strategies essential to demographic data exchange and data synchronization. Additionally, we continue to make progress toward simplifying registration and enrollment of veterans, as well as the way we manage contact with veterans throughout their lifetime.

DoD data is delivered to VBA via secure transmission, using commercial software products and a direct computer-to-computer connection. The software is called Connect:Direct Secure+, and is a file transfer utility that has enhanced security options such as mutual authentication, data encryption, and cryptographic message integrity checking. We use this software when sending and receiving files from the Defense Manpower Data Center (DMDC).

VA is fully committed to the uninterrupted delivery of benefits to those who are returning or have returned from the battlefield and are transitioning into our VA system. We recognize the importance of securing the information shared with our DoD partners.

Our mission is to serve veterans and to provide benefits to the best of our ability. IT is an essential tool that helps us serve veterans better, faster, and more thoroughly. However, the rapid rate of technological advances, while offering improved and expanded benefits delivery, also presents an ongoing challenge to VA to keep pace with security and privacy demands. IT can make our service better and faster, but the vulnerabilities increase just as fast. We must and will do what is necessary to protect, as well as to serve, our veterans.

Chairman Miller and Chairman Boozman, this concludes my statement. I would be happy to answer questions you or members of the Subcommittees might have.

STATEMENT OF
MICHAEL L. STALEY
ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE
SUBCOMMITTEE ON DISABILITY ASSISTANCE AND MEMORIAL AFFAIRS
SUBCOMMITTEE ON ECONOMIC OPPORTUNITY
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES

Hearing on Veterans Benefits Administration Data Security

June 20, 2006

Chairman Miller, Chairman Boozman, and Members of the Subcommittees, thank you for the opportunity to testify today concerning the Office of Inspector General's (OIG) reports addressing information security weaknesses in the Department of Veterans Affairs (VA) and data security practices and policies in the Veterans Benefits Administration (VBA). I will provide a general overview of our work in this area and then focus on specific issues involving VBA. In preparing this testimony, we drew on previous reports related to VA's Consolidated Financial Statements (CFS) audits since fiscal year (FY) 1997, Federal Information Security Management Act (FISMA) reviews since FY 2001, and security weaknesses and vulnerabilities at VA regional offices where security issues were evaluated during our Combined Assessment Program (CAP) reviews since FY 2000. All of these findings impact on VBA.

EXECUTIVE SUMMARY

For many years, significant concerns have been raised about VBA's information security. As part of the CFS audit, information technology (IT) security controls have been reported as a material weakness. We have reported that program and financial data are at risk due to serious problems related to control and oversight of access to information systems. We have reported segregation of duties, service continuity, and change controls need to be strengthened. Our FISMA reviews highlight specific vulnerabilities that can be exploited, but the recurring themes in these reports are the need for centralization, remediation, and accountability in VA information security. Since the FY 2001 report, we reported weaknesses in physical security, electronic security, and FISMA reporting, and since 2002, we also reported weaknesses in wireless security and personnel security. In addition to our CFS audits and FISMA reviews, our CAP reviews disclosed IT and security deficiencies at 37 (67 percent) of 55 VBA facilities reviewed. To ensure that security issues identified during audits and reviews were adequately addressed, we recommended that VA pursue a more centralized approach, apply appropriate resources, and establish a clear chain of command and accountability structure to implement and enforce IT internal controls.

Consolidated Financial Statement Audits Continue to Report Information Security as a Material Weakness

Pursuant to the Chief Financial Officers Act of 1990, the VA consolidated financial statements are audited annually. We contract with an independent public accounting firm to perform this audit. The contractor follows Government Accountability Office methodology to assess the effectiveness of computer controls at VA's three information technology centers (ITCs) and selected regional offices and medical centers.

As part of the CFS audit, IT security controls have been reported as a material weakness for many years. A material weakness is defined as a weakness in internal control that could have a material effect on the financial statements and not be detected by employees in the normal course of their business. We have reported that VA's program and financial data are at risk due to serious problems related to VA's control and oversight of access to its information systems. For example, by not controlling and monitoring employee access, not restricting users to only need-to-know data, and not timely terminating accounts upon employee departure, VA has not mitigated the potential risk. These conditions place sensitive information, including financial data and sensitive veteran medical and benefit information, at risk, possibly without detection of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As a result of these vulnerabilities, we recommended that VA pursue a more centralized approach, apply appropriate resources, and establish a clear chain of command and accountability structure to implement and enforce IT internal controls. We also recommended that VA continue its efforts to accomplish the following key tasks:

- Improve access control policies and procedures for configuring security settings on operating systems, improve administration of user access, and detect and resolve potential access violations.
- Evaluate user functional access needs and system access privileges to support proper segregation of duties within financial applications. Assign, communicate, and coordinate responsibility for enforcing and monitoring such controls consistently throughout VA.
- Develop a service continuity plan at the departmental level that will facilitate effective communication and implementation of overall guidance and standards, and provide coordination of VA's service continuity effort. Schedule and adequately test IT disaster recovery plans to ensure continuity of operations in the event of a disruption of service.
- Develop a change control framework and, within that framework, implement application specific change control procedures for mission critical systems.

VA has implemented some recommendations for specific locations identified but has not made corrections VA-wide. For example, we found violations of password policies which management immediately corrected, but in following years, we found similar violations at other facilities. We also found instances of terminated or separated employees with access to critical systems identified at various locations which management corrected, only to discover similar instances elsewhere.

Annual Evaluations of VA's Information Security Program Have Identified Vulnerabilities that Remain Uncorrected

FISMA requires us to annually review the progress of the information technology and security program of the Department and report the results to the Office of Management and Budget (OMB). As part of the FISMA review, we conduct scanning and penetration tests of selected VA systems to assess controls for monitoring and accessing systems, and reviews of physical, personnel, and electronic security. We visit the three major IT centers and selected regional offices and medical centers in addition to IT work on financial statements.

In all four audits of the VA Information Security Program issued since 2001, we reported vulnerabilities that continue to need management attention. These reports highlight specific vulnerabilities that can be exploited, but the recurring themes in these reports are the need for centralization, remediation, and accountability in VA information security. Since the FY 2001 report, we reported weaknesses in physical security, electronic security, and FISMA reporting, and since 2002, we also reported weaknesses in wireless security and personnel security. Additionally, we have reported significant issues with implementation of security initiatives VA-wide. The status of unimplemented recommendations was discussed in subsequent audits.

The FY 2004 audit also emphasized the need to centralize the IT security program, implement security initiatives, and close security vulnerabilities. We previously recognized that the Office of the Assistant Secretary for Information and Technology/Chief Information Officer's (CIO's) office needed to be fully staffed, and that funding delays and resistance by offices to relinquish their own security functions and activities delayed implementation of the fully centralized CIO contemplated by our prior recommendations. The CIO's comments to the report referenced an April 2004 VA General Counsel opinion that held the CIO lacked the authority to enforce compliance with the VA information security program as one reason he could not address vulnerabilities. We again recommended that VA fully implement and fund a centralized VA-wide IT security program.

In total, the FY 2004 report included 16 recommendations: (1) centralize IT security programs; (2) implement an effective patch management program; (3) address security vulnerabilities of unauthorized access and misuse of sensitive information and data throughout VA demonstrated during OIG field testing; (4) ensure position descriptions contain proper data access classification; (5) obtain timely, complete background investigations; and complete the following security initiatives on (6) intrusion detection systems, (7) infrastructure protection actions, (8) data center contingency planning, (9) certification and accreditation of systems, (10) upgrading/terminating external connections, (11) improvement of configuration management, (12) moving VA Central Office (VACO) data center, (13) improvement of application program/operating system change controls, (14) limiting physical access to computer rooms, (15) wireless devices, and (16) electronic transmission of sensitive veteran data. As of June 19, 2006, all recommendations from this report remain open.

CAP Reviews Show Information System Security Vulnerabilities Continue to Exist

We continue to identify instances where out-based employees send veterans' medical information to the VA regional office via unencrypted e-mail; system access for separated employees is not terminated; monitoring remote network access and usage does not routinely

occur; and off duty users' access to VA computer systems and sensitive information is not restricted. We continue to make recommendations to improve security and contingency plans, control access to information systems, complete background investigations and annual security awareness training, and improve physical security controls.

While individual and regional managers have concurred with these CAP recommendations, and our follow-up process confirms actions to resolve the specific conditions identified at these sites, we continue to find that corrective actions are not applied to all facilities to correct conditions nationwide. Consequently, we continue to find these systemic conditions at other sites we visit. For example, between FYs 2000 to 2005, we identified IT and security deficiencies at 37 (67 percent) of 55 VBA facilities reviewed.

IT Security Remains a Major Management Challenge

The OIG annually summarizes the most serious management problems identified during reviews. We have identified information security and security of data and data systems in all major management challenge reports issued since FY 2000. The major management challenges are published in VA's annual Performance and Accountability Report.

STATUS OF CURRENT FISMA RECOMMENDATIONS

We have recently issued an advance copy our of FY 2005 FISMA draft report to the Department. We restructured the draft report to respond to the Department's comments and announced reorganization actions designed to implement centralization in the CIO's office. While the OIG does not release draft reports, because of the extensive public interest in these issues resulting from the recent data loss incident involving the burglary of a VA data analyst's home, I would like to summarize the findings and recommendations of this report.

VA is still in the process of addressing recommendations made during prior FISMA audits to improve IT operations and controls. We have one additional recommendation for an existing area that needs to be elevated for priority attention. VA has made progress during FY 2005 to improve IT controls and to implement some recommendations. For example, after the FY 2005 testing was finished, VA informed us that certification and accreditation reviews have been completed and the deployment of intrusion detection systems (IDS) has been accomplished. We will validate implementation in future annual FISMA audits.

I will discuss in greater detail the 16 issues and discuss 1 new issue, as well as our recommendations for corrective actions.

Issue 1: Implementation of a Centralized Agency-wide IT Security Program

The CIO is VA's focal point for IT topics. Although the CIO is responsible for VA's information systems, operational controls were decentralized among each administration within VA. The operational control has been vested with the Veterans Health Administration (VHA), VBA, the National Cemetery Administration (NCA), and other program offices in VA. The CIO provided guidance and the tools to support the activities with operational control to secure VA systems, but the CIO did not have the ability to enforce or hold officials accountable for non-compliance. The CIO was responsible for the general management of all VA IT resources,

including policy guidance, budgetary review, and general oversight. However, the implementation of the information security program was accomplished by VA personnel who were not under the direct supervision or control of the CIO.

Recently, Congress gave VA and the CIO a unique opportunity to centralize IT operational and maintenance activities, and to establish and implement policies designed to standardize IT functionality within the Department. For example, the House in November 2005 passed H.R. 4061, known as the *"Department of Veterans Affairs Information Technology Management Improvement Act of 2005."* This bill would give the VA CIO the authority to centralize IT operations and activities consistent with one of our open recommendations.

VA informed Congress that it plans to move towards a "federated IT system" to realign department-wide IT operations and maintenance responsibilities under the direct authority of the CIO. The main feature of the realignment will place VA's IT budget, along with IT professionals involved in operation and maintenance work, directly under the authority of the Assistant Secretary for Information and Technology/CIO. However, IT employees involved in system development will remain under their respective administrations and staff offices (e.g., VHA, VBA, NCA, and some program offices). Given that the planned realignment has just begun, VA's "federated IT system" implementation plans will need further study. For example, we will need to review whether existing IT systems and operations under the purview of the CIO will efficiently and effectively communicate with newly designed applications implemented by these system development offices. Failure to implement sound policies and procedures could introduce a significant amount of risk into the production environment if the access controls given to development staffs are not adequately developed and enforced.

Issue 2: Implementation of a Patch Management Program

VA continues to review and address patch management issues to find long-term solutions. We previously identified a number of critical patches that were either not installed or not appropriately implemented at the VA facilities reviewed. VA did not have an enterprise-wide solution that could directly connect to over 250,000 points within VA, including VBA desktops on which VBA employees ran e-mail. During our FY 2005 review, VA continued to evaluate solutions to remediate this condition. VA was still in the process of developing and fully deploying a patch management program.

VA's CIO identified roles and responsibilities to address VA Enterprise Patch Management processes and standard operating procedures. A January 7, 2005, memorandum, *Enterprise Patch Management,* signed by the CIO, details patch management roles, responsibilities, and special considerations. We are continuing to follow up on the efforts taken by VA to implement this recommendation in future audits.

Issue 3: Electronic Security

Our reviews conducted at Hines and Philadelphia ITCs, the Chicago Regional Office, and the Philadelphia Regional Office and Insurance Center during FY 2005 found potential vulnerabilities that we previously identified relating to password controls, remote access, and securing critical files. Additionally, we continued to find security vulnerabilities related to the

lack of segregation of duties; unsecured critical files, which could allow attackers access to password files; and inappropriate access through remote access software.

Our field work at facilities previously visited in prior years—including the Washington, D.C, Regional Office—found potential vulnerabilities warranting management attention. The reviews indicate that while managers at sites visited are addressing vulnerabilities identified during these reviews, sites not visited in prior years have not been advised that the vulnerabilities identified may be systemic in nature. VA needs a consistent approach at all of its facilities to effectively monitor networks and to use tools, such as electronic scanning, to proactively identify and correct security vulnerabilities.

Issue 4: Personnel Security

In FY 2005, we continued to find previously identified weaknesses related to position descriptions and training of VA employees and contractors, including those in VBA. Sensitive position descriptions needed better documentation. We found the sensitivity rating was inaccurate for some employee positions at facilities reviewed and that position descriptions needed to more specifically address the levels of access relative to the positions' duties and responsibilities. To ensure the integrity of the benefits program, OIG recommended that VBA employees disclose in writing their own and their relatives' veteran status. We continue to identify lack of compliance with this requirement.

Issue 5: Background Investigations

VBA needs to ensure that employee and contractor background investigation requirements are adequately identified and addressed. In FY 2005, we identified instances where background investigations and reinvestigations were not initiated in a timely manner on employees and contractors, or were not initiated at all. We will follow up on this issue in future FISMA audits.

Issue 6: Deployment and Installation of Intrusion Detection Systems

Although much has been done, the VA's Office of Cyber and Information Security (OCIS) still need to validate whether VA completed installation of IDS at all sites, including VBA sites. Deploying and installing IDS is a key step in the process of securing VA data systems on a national basis. Implementation of IDS increases VA's ability to detect intrusions. OCIS advised us that an enterprise-wide IDS has been fully implemented. In addition, OCIS is researching the benefits of moving to Intrusion Prevention Systems in an effort to provide VA the capability to detect and prevent "attacks." We will be testing the effectiveness of the IDS system in future FISMA audits.

Issue 7: Infrastructure Protection Actions

VA needs to complete infrastructure planning efforts. During our FY 2004 audit, we found examples where the physical infrastructure had significant vulnerabilities and did not adequately protect data from potential destruction, manipulation, and inappropriate disclosure. During our FY 2005 field work, we found that VA was developing a Critical Infrastructure Protection Plan, and completed an identification and prioritization of critical information resources. We will

review VA's progress in completing and implementing this plan in future FISMA audits. Specific VBA vulnerabilities include perimeter security, old hardware, and legacy applications.

Issue 8: Information Technology Centers' Continuity of Operations Plans

VBA is making progress and had completed Continuity of Operations (COOP) plans but full testing needs to be done. VA has issued an Emergency Preparedness Directive/Handbook 0320 for the VACO's COOP. VA was developing a Master COOP for the entire VA, which will include all elements in the Central Office COOP. National Institute of Standards and Technology (NIST) 800-34, *Contingency Planning Guide for Information Technology Systems,* dated June 2002, recommends COOP testing should be accomplished at least annually. COOPs covering ITCs need to ensure capabilities exist to provide necessary operational support in the event of disasters.

Our field tests conducted in FY 2005 showed that the ITCs have completed these contingency plans, but that testing these plans needed to be jointly done among all program offices residing in the ITCs. After FY 2005 field work was completed, we learned that VBA-related hardware had been procured at one ITC to back up data, and some independent testing has been performed. For example, VBA informed us that they recently conducted tests at their ITCs and performed disaster recovery exercises. While this is a step forward, joint collaborative testing by all tenant offices within the ITCs (VHA, VBA, NCA, and other offices) would serve as a better gauge of determining the adequacy of responses. We will follow up on this issue in future FISMA audits.

Issue 9: Certification and Accreditation Process

During FY 2005 field work, we found that VA had placed a priority on the uncompleted Certification and Accreditation (C&A) process. The number of VA systems and major applications decreased from 678 in FY 2004 to 585 in FY 2005, as a result of VA combining applications or by removing previously reported systems that did not meet the NIST criteria. VBA has 96 of the 585 systems and major applications. At the end of our field work in the summer of 2005, VA had not completed a C&A for all systems and major applications. The former Secretary of Veterans Affairs had made it a priority to complete all C&A work by the end of August 2005, and in November 2005, VA reported to OMB that it had completed a C&A for all VA systems and major applications. We will follow up in future FISMA audits to ensure all C&A work has been done, that self-reported deficiencies have been identified and actions are underway to address them, and that there is documentation to support the C&A work.

Issue 10: Terminate/Upgrade External Connections

In prior audits, we reported security risks associated with the operation of uncertified Internet gateways that affect the entire Department, including VBA. As of FY 2005, VA took actions to mitigate these risks by limiting the number of Internet gateways in order to improve control over access to VA systems.

Field work conducted in FY 2005 found that VA is still unable to determine if all extraneous external connections have been terminated. We are currently unsure of the extent VA and its affiliated and non-affiliated partners may be operating their own gateways.

We also found that the standard contract VA used to procure computers included as a standard feature, modem devices, which if retained in default settings could serve as access points for hackers attempting to gain entry into VA systems. A January 2005 OIG report on procurement of desktop modems prompted VA to amend its contract and to address the modem security vulnerabilities with all facilities. We have left this recommendation open and will be continuing to review this issue during future FISMA audits.

Issue 11: Configuration Management

Prior year audits have found instances where VA networks relied on old operating systems such as Windows 95 and Windows 98, which placed the VA networks at risk due to the lack of vendor support to upgrade security and other features. An unsupported operating system, whether desktop or production mainframe, exposes VA to potential security and operational risks, including operating system failure.

During FY 2005 field work, we found VBA had reduced the number of personal computers running Windows 95, but other aged computers must continue to operate due to special document scanners associated with The Imaging Management System (known as "TIMS"). We were told that these scanners and personal computers are expected to be replaced or retired during FY 2006, if funds are available. The System Configuration and Management Program continues to review this issue, however, actions are still pending completion; therefore, we will follow up on future audits.

Issue 12: Movement and Consolidation of VACO's Data Center

We previously reported that the VACO data center was located below ground level and experienced water damage twice in the last 10 years. This facility houses the hardware that supports the VBA headquarters operation. VA reported the relocation of the VACO data center is in progress. In the interim, VA placed equipment in multiple locations throughout the Washington, D.C., metropolitan area until procurement and construction is completed at a new location. Even though progress has been made, our observations identified routers and switches that support VACO network backbone critical to their operations remain below ground level. We will follow up on this issue in future FISMA audits.

Issue 13: Application Program/Operating System Change Controls

VA change control policy does not provide uniform application development and change guidance for a wide range of new and legacy applications, including VBA systems. Nationwide policy is necessary to facilitate consistent implementation and effective monitoring of system change controls for mission critical systems.

For example, we found changes to a mainframe operating system and supporting hardware were not supported by local management authorization. Additionally, we found instances where changes to the production environment were not adequately documented or approved for major applications and critical systems. Consequently, unauthorized changes could have adversely affected the production environment or lead to misuse without warning. We will continue to follow up on this issue in future FISMA audits.

Issue 14: Physical Access Controls

At previous sites visited, VBA was attempting to make improvements to ensure adequate measures were implemented to secure veterans' information and provide a safe environment for employees and visitors. However, our facility reviews at new locations showed physical access controls still need improvement. For example, a number of facilities granted access to computer rooms to employees who did not have a need to be in the computer room to perform their job function, and some contractors did not have an escort while in the computer room. We will continue to follow up on this issue in future FISMA audits.

Issue 15: Wireless Security

VA is making progress in reducing wireless security vulnerabilities by securing its network from outside intrusion. Actions were taken to install an encryption wireless product that is designed to prohibit unauthorized users from accessing the network. However, our contractor penetration test showed some vulnerability in the wireless network could be used to view transmissions, including location of veterans' claims folders, and to gain access to systems residing on VA's internal networks. Despite improvements, VA's information systems remained at risk for unauthorized access or misuse of sensitive information.

Issue 16: Encrypting Sensitive Information on VA Networks

VA has stated that it was taking interim steps to improve transmission of protected and sensitive information over its networks as sensitive data continues to be transmitted in clear text on VA networks. VA informed us that installation of encryption capabilities on some of its older platforms would render the systems inefficient. The OIG contractor penetration team was able to access regional office files, create a fictitious veteran, establish an award, and mail an award letter to a real address as a trusted insider as a result of unencrypted information. Our site work also showed that unencrypted protected benefit information was vulnerable within VA.

Issue 17: FISMA Reporting Database

FISMA establishes security requirements and requires VA to annually report vulnerabilities for systems and major applications. While VBA is taking actions to address security vulnerabilities, we continue to identify weaknesses that require a centralized and coordinated effort to ensure corrective actions are taken to control access, to secure computer rooms, and to ensure facilities accurately report their security deficiencies that place VBA information and data at risk.

The FISMA database[1] contains the self-assessment surveys of VBA's major applications and systems. System and application deficiencies, as well as funded and unfunded remediation plans, are reported and stored in this database. Consequently, this database needs to accurately demonstrate the security posture of VBA's systems and major applications. Also, it should accurately depict the risk of loss of the critical and sensitive information contained within these systems and major applications.

[1] In FY 2006, the FISMA database became known as the Security Management and Reporting Tool (SMART) database.

Comparisons of the sites visited to the entries in the FISMA database found that not all information was accurate or complete. Most inaccuracies involved reporting of the five levels of IT security program effectiveness outlined in the Federal Information Technology Security Assessment Framework. Additionally, facilities were not held accountable for information inaccuracies or incomplete data in the database. For example, fields requiring information pertaining to the amount of funding needed to correct deficiencies were incomplete. VBA senior leadership needs this information to determine the costs to correct the conditions identified. With inaccurate or incomplete information in the FISMA database, VA senior leadership will not have a complete picture of VA's information security posture and the level of resources and funding needed to remediate security deficiencies.

RECOMMENDATIONS

We recommended that the Acting Assistant Secretary for Information and Technology/CIO, in conjunction with senior VA leadership, take actions to fully address all 17 issues summarized above.

CLOSING

In closing, I would like the Subcommittees to know that reviews of VA's information security will remain a priority for the OIG until these issues are resolved. We remain committed to following up and continuing to assess the adequacy of IT controls with the resources that are available, and we will remain dedicated to the goal of protecting our Nation's veterans. Our efforts will include protection of data maintained by VBA as one of the major VA components.

Chairman Miller, Chairman Boozman, and Members of the Subcommittees, thank you again for this opportunity to provide you the status of our work. I am available to answer any questions.

United States Government Accountability Office

GAO

Testimony

Before the Subcommittees on Disability Assistance and Memorial Affairs and on Economic Opportunity, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at time 10:00 a.m. EDT
June 20, 2006

INFORMATION SECURITY

Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs

Statement of Linda D. Koontz
Director, Information Management Issues

and

Gregory C. Wilshusen
Director, Information Security Issues

GAO-06-897T

June 20 2006

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-06-897T, a testimony before the Subcommittees on Disability Assistance and Memorial Affairs and on Economic Opportunity, Committee on Veterans' Affairs, House of Representatives

INFORMATION SECURITY

Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs

Why GAO Did This Study

The recent information security breach at the Department of Veterans Affairs (VA), in which personal data on millions of veterans were compromised, has highlighted the importance of the department's security weaknesses, as well as the ability of federal agencies to protect personal information. Robust federal security programs are critically important to properly protect this information and the privacy of individuals.

GAO was asked to testify on VA's information security program, ways that agencies can prevent improper disclosures of personal information, and issues concerning notifications of privacy breaches. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources.

What GAO Recommends

To ensure that security and privacy issues are adequately addressed, GAO has made recommendations previously to VA and other agencies on implementing federal privacy and security laws. In addition, GAO has previously testified that in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

www.gao.gov/cgi-bin/getrpt?GAO-06-897T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

For many years, significant concerns have been raised about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information, including sensitive personal information. GAO and the department's inspector general have reported recurring weaknesses throughout VA, including the Veterans Benefits Administration, in such areas as access controls, physical security, and segregation of incompatible duties. The department has taken steps to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. For example, it is still developing plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. Without an established and implemented security program, the department will continue to have major challenges in protecting its information and information systems from security breaches such as the one it recently experienced.

In addition to establishing robust security programs, agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. A key step is to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed—whenever information technology is used to process personal information. In addition, agencies can take more specific practical measures aimed at preventing data breaches, including limiting the collection of personal information, limiting the time that such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on portable devices.

When data breaches do occur, notification of those affected and/or the public has clear benefits, allowing people the opportunity to protect themselves from identity theft. Although existing laws do not require agencies to notify the public of data breaches, such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection. That said, care is needed in defining appropriate criteria for triggering notification. Notices should be coordinated with law enforcement to avoid impeding ongoing investigations, and in order to be effective, notices should be easy to understand. Because of the possible adverse impact of a compromise of personal information, it is critical that people fully understand the threat and their options for addressing it.

Strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight will be needed for VA to address its persistent, long-standing control weaknesses.

Messers. Chairmen and Members of the Subcommittees:

Thank you for inviting us to participate in today's hearing on information security and privacy at the Department of Veterans Affairs (VA). For many years, we have identified information security as a governmentwide high-risk issue[1] and emphasized its criticality for protecting the government's information assets. The recent security breach at VA, involving the loss of personal data on millions of veterans, also raises important questions about the protection of personally identifiable information.[2]

Today we will first address VA's information security program, including weaknesses reported by us and others, as well as actions that VA has taken to address past recommendations in this area. We will then discuss potential measures that federal agencies can take to help limit the likelihood of personal information being compromised. Finally, we will highlight key benefits and challenges associated with effectively notifying the public about security breaches.

To describe VA's information security weaknesses, we reviewed our previous work in this area, as well as reports by VA's inspector general (IG) and others. To determine the implementation status of our open recommendations, we analyzed VA documentation and met with officials from VA, including security and IG officials. To address measures that agencies can take to help limit the likelihood of personal information being compromised, we identified and summarized issues raised by experts in congressional testimony and in our previous reports, including our recent work regarding the federal government's use of personal information from companies

[1] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005) and *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[2] For purposes of this testimony, the term *personal information* encompasses all information associated with an individual, including both identifiable and nonidentifying information. *Personally identifiable information*, which can be used to locate or identify an individual, includes such things as names, aliases, and Social Security numbers. *Nonidentifying personal information* includes such things as age, education, finances, criminal history, physical attributes, and gender.

known as information resellers.[3] To identify benefits and challenges associated with effectively notifying the public about security breaches, we reviewed our previous work in this area. We conducted the work for our previous reports in accordance with generally accepted government auditing standards. To provide additional information on our previous work related to VA security issues and to privacy, we have included, as an attachment, a list of pertinent GAO publications.

Results in Brief

Significant concerns have been raised over the years about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information. We have previously reported on wide-ranging deficiencies in VA's information security controls.[4] For example, the department lacked effective controls to prevent individuals from gaining unauthorized access to VA systems and sensitive information, and it had not consistently provided adequate physical security for its computer facilities, assigned duties in a manner that segregated incompatible functions, controlled changes to its operating systems, or updated and tested its disaster recovery plans. These deficiencies existed, in part, because VA had not fully implemented key components of a comprehensive, integrated information security program. Although VA has taken steps to implement components of its security program, its efforts have not been sufficient to effectively protect its information and information systems. As a result, sensitive information, including personally identifiable information, remains vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure, as the recent breach demonstrates.

[3] GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington: D.C.: Apr. 4, 2006).

[4] See attachment 1.

In addition to establishing a robust information security program, agencies can take a number of actions to help protect personally identifiable information from compromise. A key step is to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed in a federal information system—whenever information technology is used to process personal information. In addition, specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting data retention, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on portable devices.

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. It is also consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and promotes accountability for its protection. If agencies are required to report security breaches to the public, care will be needed to develop appropriate criteria for incidents that require notification. Care is also needed to ensure that notices are useful and easy to understand, so that they are effective in alerting individuals to actions they may want to take to minimize the risk of identity theft.

We have made recommendations previously to VA regarding information security and to the Office of Management and Budget (OMB) and agencies regarding privacy issues, including the conduct of privacy impact assessments. In addition, we have previously testified that the Congress should consider setting specific reporting requirements for agencies as part of its consideration of security breach legislation. Further, the Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to affected individuals.

Background

Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous, but without proper safeguards in the form of appropriate information security, this widespread interconnectivity also poses significant risks to the government's computer systems and the critical operations and infrastructures they support.

In prior reviews we have repeatedly identified weaknesses in almost all areas of information security controls at major federal agencies, including VA, and we have identified information security as a high risk area across the federal government since 1997. In July 2005, we reported that pervasive weaknesses in the 24 major agencies' information security policies and practices threatened the integrity, confidentiality, and availability of federal information and information systems.[5] As we reported, although federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. These weaknesses existed primarily because agencies had not yet fully implemented strong information security programs, as required by the Federal Information Security Management Act (FISMA).

The significance of these weaknesses led us to conclude in the audit of the federal government's fiscal year 2005 financial statements[6]

[5] GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[6] U.S. Department of the Treasury, *Financial Report of the United States Government 2005* (Washington, D.C.: 2005).

that information security was a material weakness.[7] Our audits also identified instances of similar types of weaknesses in nonfinancial systems. Weaknesses continued to be reported in each of the major areas of *general controls:* that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.[8]

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, without which agencies would find it difficult, if not impossible, to carry out their missions and account for their resources. The following examples show the broad array of federal operations and assets placed at risk by information security weaknesses:

- Resources, such as federal payments and collections, could be lost or stolen.
- Computer resources could be used for unauthorized purposes or to launch attacks on others.
- Personal information, such as taxpayer data, social security records, and medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of identity theft, industrial espionage, or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.
- Data could be modified or destroyed for purposes of fraud, theft of assets, or disruption.
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

[7] A material weakness is a condition that precludes the entity's internal control from providing reasonable assurance that misstatements, losses, or noncompliance that is material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

[8] The main areas of general controls are an agencywide security program, access controls, software change controls, segregation of duties, and continuity of operations planning.

The potential disclosure of personal information raises additional identity theft and privacy concerns. Identity theft generally involves the fraudulent use of another person's identifying information—such as Social Security number, date of birth, or mother's maiden name—to establish credit, run up debt, or take over existing financial accounts. According to identity theft experts, individuals whose identities have been stolen can spend months or years and thousands of dollars clearing their names. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft. The Federal Trade Commission (FTC) reported in 2005 that identity theft represented about 40 percent of all the consumer fraud complaints it received during each of the last 3 calendar years. Beyond the serious issues surrounding identity theft, the unauthorized disclosure of personal information also represents a breach of individuals' privacy rights to have control over their own information and to be aware of who has access to this information.

Key Laws Govern Agency Security and Privacy Practices

Federal agencies are subject to security and privacy laws aimed in part at preventing security breaches, including breaches that could enable identity theft.

FISMA is the primary law governing information security in the federal government; it also addresses the protection of personal information in the context of securing federal agency information and information systems. The act defines federal requirements for securing information and information systems that support federal agency operations and assets.[9] Under FISMA, agencies are required to provide sufficient safeguards to cost-effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure (and thus to protect personal privacy, among other things). The act requires each agency to develop, document, and implement an agencywide information security program to provide

[9] FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

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.

FISMA describes a comprehensive information security program as including the following elements:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce risks to an acceptable level and ensure that security is addressed throughout the life cycle of each information system;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies through plans of action and milestones; and
- procedures for detecting, reporting, and responding to security incidents.

In particular, FISMA requires that for any information they hold, agencies evaluate the associated risk according to three categories: (1) confidentiality, which is the risk associated with unauthorized disclosure of the information; (2) integrity, the risk of unauthorized modification or destruction of the information; and (3) availability, which is the risk of disruption of access to or use of information. Thus, each agency should assess the risk associated with personal data held by the agency and develop appropriate protections.

The agency can use this risk assessment to determine the appropriate controls (operational, technical, and managerial) that will reduce the risk to an acceptably low level. For example, if an agency assesses the confidentiality risk of the personal information as high, the agency could create control mechanisms to help protect the data from unauthorized disclosure. Besides appropriate policies,

these controls would include access controls and monitoring systems:

- Access controls are key technical controls to protect the confidentiality of information. Organizations use these controls to grant employees the authority to read or modify only the information the employees need to perform their duties. In addition, access controls can limit the activities that an employee can perform on data. For example, an employee may be given the right to read data, but not to modify or copy it. Assignment of rights and permissions must be carefully considered to avoid giving users unnecessary access to sensitive files and directories.
- To ensure that controls are, in fact, implemented and that no violations have occurred, agencies need to monitor compliance with security policies and investigate security violations. It is crucial to determine what, when, and by whom specific actions are taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security events.

A comprehensive security program of the type described is a prerequisite for the protection of personally identifiable information held by agencies. In addition, agencies are subject to requirements specifically related to personal privacy protection, which come primarily from two laws, the Privacy Act of 1974 and the E-Government Act of 2002.

- The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act

requires that when agencies establish or make changes to a system of records, they must notify the public by a "system-of-records notice": that is, a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.[10] Among other provisions, the act also requires agencies to define and limit themselves to specific predefined purposes.

The provisions of the Privacy Act are consistent with and largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices,[11] which have been widely adopted as a standard benchmark for evaluating the adequacy of privacy protections; they include such principles as openness (keeping the public informed about privacy policies and practices) and accountability (those controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles).

- The E-Government Act of 2002 strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,[12] a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in

[10] Under the Privacy Act of 1974, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[11] These principles were first proposed in 1973 by a U.S. government advisory committee; they were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

[12] Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. To the extent that PIAs are made publicly available,[13] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

Interest in Data Breach Notification Legislation Has Increased

Federal laws to date have not required agencies to report security breaches to the public,[14] although breach notification has played an important role in the context of security breaches in the private sector. For example, requirements of California state law led ChoicePoint, a large information reseller,[15] to notify its customers of a security breach in February 2005. Since the ChoicePoint notification, bills were introduced in at least 44 states and enacted in at least 29[16] that require some form of notification upon a security breach.

A number of congressional hearings were held and bills introduced in 2005 in the wake of the ChoicePoint security breach as well as incidents at other firms. In March 2005, the House Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy

[13] The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. 107-347, § 208(b)(1)(B)(iii).

[14] At least one agency has developed its own requirement for breach notification. Specifically, the Department of Defense instituted a policy in July 2005 requiring notification to affected individuals when protected personal information is lost, stolen, or compromised.

[15] Information resellers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which include both private-sector businesses and government agencies. For additional information, see GAO-06-421.

[16] States that have enacted breach notification laws include Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin.

and Commerce Committee held a hearing entitled "Protecting Consumers' Data: Policy Issues Raised by ChoicePoint," which focused on potential remedies for security and privacy concerns regarding information resellers. Similar hearings were held by the House Energy and Commerce Committee and by the U.S. Senate Committee on Commerce, Science, and Transportation in spring 2005.

Several bills introduced at the time of these hearings, such as the Data Accountability and Trust Act (DATA),[17] would establish a national requirement for companies that maintain personal information to notify the public of security breaches. In May 2006, DATA was amended to also require federal agencies to notify citizens and residents of the United States whose personal information is acquired by an unauthorized person as a result of a security breach. Other bills under consideration also include federal agencies. For example, the Notification of Risk to Personal Data Act[18] would require federal agencies as well as any "persons engaged in interstate commerce" to disclose security breaches involving unauthorized acquisition of personal data.

VA's Information Security Is Weak

Our previous reports and testimonies describe numerous weaknesses in VA's information security controls, including those at the Veterans Benefits Administration. Although the department has taken steps to address these weaknesses, they have not been sufficient to fully implement a comprehensive, integrated information security program and to fully protect VA's information and information systems. As a result, these remain at risk.

[17] H.R. 4127; introduced by Representative Clifford B. Stearns on October 25, 2005.

[18] S. 751; introduced by Senator Dianne Feinstein on April 11, 2005.

VA's Information Security Weaknesses Are Long Standing

In carrying out its mission of providing health care and benefits to veterans, VA relies on a vast array of computer systems and telecommunications networks to support its operations and store sensitive information, including personal information on veterans. VA's networks are highly interconnected, its systems support many users, and the department has increasingly moved to more interactive, Web-based services to better meet the needs of its customers. Effectively securing these computer systems and networks is critical to the department's ability to safeguard its assets, maintain the confidentiality of sensitive veterans' health and disability benefits information, and ensure the integrity of its financial data.

In this complex IT environment, VA has faced long-standing challenges in achieving effective information security across the department. Our reviews[19] identified wide-ranging, often recurring deficiencies in the department's information security controls (attachment 2 provides further detail on our reports and the areas of weakness they discuss). Examples of areas of deficiency include the following.

- *Access authority was not appropriately controlled.* A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Electronic access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information and include controls related to user accounts and passwords, user rights and file permissions, logging and monitoring of security-relevant events, and network management. Inadequate controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service.

[19] Attachment 1 includes a list of our products related to IT vulnerabilities at VA.

However, VA had not established effective electronic access controls to prevent individuals from gaining unauthorized access to its systems and sensitive data, as the following examples illustrate:

- *User accounts and passwords*: In 1998, many user accounts at four VA medical centers and data centers had weaknesses including passwords that could be easily guessed, null passwords, and passwords that were set to never expire. We also found numerous instances where medical and data center staff members were sharing user IDs and passwords.
- *User rights and permissions:* We reported in 2000 that three VA health care systems were not ensuring that user accounts with broad access to financial and sensitive veteran information had proper authorization for such access, and were not reviewing these accounts to determine if their level of access remained appropriate.
- *Logging and monitoring of security-related events:* In 1998, VA did not have any departmentwide guidance for monitoring both successful and unsuccessful attempts to access system files containing key financial information or sensitive veteran data, and none of the medical and data centers we visited were actively monitoring network access activity. In 1999, we found that one data center was monitoring failed access attempts, but was not monitoring successful accesses to sensitive data and resources for unusual or suspicious activity.
- *Network management:* In 2000, we reported that one of the health care systems we visited had not configured a network parameter to effectively prevent unauthorized access to a network system; this same health care system had also failed to keep its network system software up to date.

- *Physical security controls were inadequate.* Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. VA had weaknesses in the physical security for its computer facilities. For example, in our 1998 and 2000 reports, we stated that none of the VA

facilities we visited were adequately controlling access to their computer rooms. In addition, in 1998 we reported that sensitive equipment at two facilities was not adequately protected, increasing the risk of disruption to computer operations or network communications.

- *Employees were not prevented from performing incompatible duties.* Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation. Dividing duties among two or more individuals or organizational groups diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. We determined that VA did not assign employee duties and responsibilities in a manner that segregated incompatible functions among individuals or groups of individuals. For example, in 1998 we reported that some system programmers also had security administrator privileges, giving them the ability to eliminate any evidence of their activity in the system. In 2000, we reported that two VA health care systems allowed some employees to request, approve, and receive medical items without management approval, violating both basic segregation of duties principles and VA policy; in addition, no mitigating controls were found to alert management of purchases made in this manner.

- *Software change control procedures were not consistently implemented.* It is important to ensure that only authorized and fully tested systems are placed in operation. To ensure that changes to systems are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. We found that VA did not adequately control changes to its operating systems. For example, in 1998 we reported that one VA data center had not established detailed written procedures or formal guidance for modifying operating system software, for approving and testing operating system software changes, or for implementing these changes. The data center had made more than 100 system software changes during fiscal year 1997, but none of the changes included evidence of testing, independent review, or acceptance. We reported

in 2000 that two VA health care systems had not established procedures for periodically reviewing changes to standard application programs to ensure that only authorized program code was implemented.

- *Service continuity planning was not complete.* In addition to protecting data and programs from misuse, organizations must also ensure that they are adequately prepared to cope with a loss of operational capability due to earthquakes, fires, accidents, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested service continuity plan. Such a plan is critical for helping to ensure that information system operations and data can be promptly restored in the event of a disaster. We reported that VA had not completed or tested service continuity plans for several systems. For example, in 1998 we reported that one VA data center had 17 individual disaster recovery plans covering various segments of the organization, but it did not have an overall document that integrated the 17 separate plans and defined the roles and responsibilities for the disaster recovery teams. In 2000, we determined that the service continuity plans for two of the three health care systems we visited did not include critical elements such as detailed recovery procedures, provisions for restoring mission-critical systems, and a list of key contacts; in addition, none of the health care systems we visited were fully testing their service continuity plans.

These deficiencies existed, in part, because VA had not implemented key components of a comprehensive computer security program. Specifically, VA's computer security efforts lacked

- clearly delineated security roles and responsibilities;
- regular, periodic assessments of risk;
- security policies and procedures that addressed all aspects of VA's interconnected environment;
- an ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; and

- a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

As a result, we made a number of recommendations in 2002 that were aimed at improving VA's security management.[20] Among the primary elements of these recommendations were that (1) VA centralize its security management functions and (2) it perform other actions to establish an information security program, including actions related to risk assessments, security policies and procedures, security awareness, and monitoring and evaluating computer controls.[21]

VA's Efforts to Address Information Security Weaknesses Have Been Limited

The department has taken steps to address the weaknesses that we described, but these have not been sufficient to fully implement a comprehensive information security program.[22] Examples of actions that VA has taken and still needs to take include the following:

- *Central security management function*: The department realigned its information technology resources to place administration and field office security functions more directly under the oversight of the department's CIO, consolidating all administration-level cyber security functions under the department's cyber security office. In addition, to provide greater management accountability for information security, the Secretary instituted information security

[20] GAO, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, GAO-02-703 (Washington, D.C.: June 12, 2002).

[21] We based our recommendations on guidance and practices provided in GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998); *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D. C.: November 1999); and Chief Information Officer Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C.: Nov. 28, 2000). FISMA (passed in late 2002) and associated guidance are generally consistent with this earlier guidance.

[22] This result is also reflected in the department's failing grade in the annual report card on computer security that is issued by the House Government Reform Committee: *Computer Security Report Card* (Washington, D.C.: Mar. 16, 2006).

standards for members of the department's senior executive service. The cyber security officer organized his office to focus more directly on critical elements of information security control, and he updated the department's security management plan and information security policies and procedures. However, the department still needed to develop policy and guidance to ensure (1) authority and independence for security officers and (2) departmentwide coordination of security functions.

- *Periodic risk assessments:* VA is implementing a commercial tool to identify the level of risk associated with system changes and also to conduct information security risk assessments. It also created a methodology that establishes minimum requirements for such risk assessments. However, it has not yet completed its risk assessment policy and guidance. VA reported that such guidance was forthcoming as part of an overarching information system security certification and accreditation policy that was to be developed during 2006. Without these elements, VA cannot be assured that it is appropriately performing risk assessments departmentwide.
- *Security policies and procedures:* VA's cyber security officer reported that VA has action ongoing to develop a process for collecting and tracking performance data, ensuring management action when needed, and providing independent validation of reported issues. VA also has ongoing efforts in the area of detecting, reporting, and responding to security incidents. For example, it established network intrusion prevention capability at its four enterprise gateways. It is also developing strategic and tactical plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. However, these plans are not complete.
- *Security awareness:* VA has taken steps to improve security awareness training. It holds an annual department information security conference, and it has developed a Web portal for security training, policy, and procedures, as well as a security awareness course that VA employees are required to review annually. However, VA has not demonstrated that it has a process to ensure compliance.
- *Monitoring and evaluating computer controls:* VA established a process to better monitor and evaluate computer controls by tracking the status of security weaknesses, corrective actions taken,

and independent validations of corrective actions through a software data base.[23] However, more remains to be done in this area. For example, although certain components of VA reported vulnerability and penetration testing to evaluate controls on internal and external access to VA systems, this testing was not part of an ongoing departmentwide program.

Since our last report in 2002, VA's IG and independent auditors have continued to report serious weaknesses with the department's information security controls. The auditors' report on internal controls,[24] prepared at the completion of VA's 2005 financial statement audit, identified weaknesses related to access control, segregation of duties, change control, and service continuity—a list of weaknesses that are virtually identical to those we identified years earlier. The department's *FY 2005 Annual Performance and Accountability Report* states that the IG determined that many information system security vulnerabilities reported in national audits from 2001 through 2004 remain unresolved, despite the department's actions to implement IG recommendations in previous audits. The IG also reported specific security weaknesses and vulnerabilities at 45 of 60 VA health care facilities and 11 of 21 VA regional offices where security issues were reviewed, placing VA at risk that sensitive data may be exposed to unauthorized access and improper disclosure, among other things. As a result, the IG determined that weaknesses in VA's information technology security controls were a material weakness.

In response to the IG's findings, the department indicates that plans are being implemented to address the material weakness in information security. According to the department, it has maximized limited resources to make significant improvement in its overall security posture in the near term by prioritizing FISMA remediation activities, and work will continue in the next fiscal year.

[23] VA's Security Management and Reporting Tool (SMART).

[24] The auditor's report is included in VA's *FY 2005 Annual Performance and Accountability Report*.

Despite these actions, the department has not fully implemented the key elements of a comprehensive security management program, and its efforts have not been sufficient to effectively protect its information systems and information, including personally identifiable information, from unauthorized disclosure, misuse, or loss.

Agencies Can Take Steps to Reduce the Likelihood That Personal Data Will Be Compromised

In addition to establishing a robust information security program, agencies can take other actions to help guard against the possibility that personal information they maintain is inadvertently compromised. These include conducting privacy impact assessments and taking other practical measures.

Conduct Privacy Impact Assessments

It is important that agencies identify the specific instances in which they collect and maintain personal information and proactively assess the means they intend to use to protect this information. This can be done most effectively through the development of privacy impact assessments (PIAs), which, as previously mentioned, are required by the E-Government Act of 2002 when agencies use information technology to process personal information. PIAs are important because they serve as a tool for agencies to fully consider the privacy implications of planned systems and data collections before those systems and collections have been fully implemented, when it may be relatively easy to make critical adjustments.

In prior work we have found that agencies do not always conduct PIAs as they are required. For example, our review of selected data mining efforts at federal agencies[25] determined that PIAs were not always being done in full compliance with OMB guidance. Similarly,

[25] GAO, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (Washington, D.C.: Aug. 15, 2005).

as identified in our work on federal agency use of information resellers,[26] few PIAs were being developed for systems or programs that made use of information reseller data, because officials did not believe they were required. Complete assessments are an important tool for agencies to identify areas of noncompliance with federal privacy laws, evaluate risks arising from electronic collection and maintenance of information about individuals, and evaluate protections or alternative processes needed to mitigate the risks identified. Agencies that do not take all the steps required to protect the privacy of personal information risk the improper exposure or alteration of such information. We recommended that the agencies responsible for the data mining efforts we reviewed complete or revise PIAs as needed and make them available to the public. We also recommended that OMB revise its guidance to clarify the applicability of the E-Gov Act's PIA requirement to the use of personal information from resellers. OMB stated that it would discuss its guidance with agency senior officials for privacy to determine whether additional guidance concerning reseller data was needed.

Employ Measures to Prevent Inadvertent Data Breaches

Besides strategic approaches such as establishing an information security program and conducting PIAs, agencies can consider a range of specific practical measures for protecting the privacy and security of personal information. Several that may be of particular value in preventing inadvertent data breaches include the following:

Limit collection of personal information. One item to be analyzed as part of a PIA is the extent to which an agency needs to collect personal information in order to meet the requirements of a specific application. Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information—such as Social Security numbers—may not be needed for many agency applications that have databases of other personal information. Limiting the collection of personal information is also one of the fair

[26] GAO-06-421, pp. 59–61.

information practices, which are fundamental to the Privacy Act and to good privacy practice in general.

Limit data retention. Closely related to limiting data collection is limiting retention. Retaining personal data longer than needed by an agency or statutorily required adds to the risk that the data will be compromised. In discussing data retention, California's Office of Privacy Protection recently reported an example in which a university experienced a security breach that exposed 15-year-old data, including Social Security numbers. The university subsequently reviewed its policies and decided to shorten the retention period for certain types of information.[27] As part of their PIAs, federal agencies can make decisions up front about how long they plan to retain personal data, aiming to retain the data for as brief a period as necessary.

Limit access to personal information and train personnel accordingly. Only individuals with a need to access agency databases of personal information should have such access, and controls should be in place to monitor that access. Further, agencies can implement technological controls to prevent personal data from being readily transferred to unauthorized systems or media, such as laptop computers, discs, or other electronic storage devices. Security training, which is required for all federal employees under FISMA, can include training on the risks of exposing personal data to potential identity theft, thus helping to reduce the likelihood of data being exposed inadvertently.

Consider using technological controls such as encryption when data need to be stored on portable devices. In certain instances, agencies may find it necessary to enable employees to have access to personal data on portable devices such as laptop computers. As discussed, this should be minimized. However, when absolutely necessary, the risk that such data could be exposed to unauthorized individuals can be reduced by using technological controls such as encryption, which significantly limits the ability of such individuals to gain access to the data. Although encrypting data adds to the

[27] State of California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information* (April 2006), p. 6.

operational burden on authorized individuals, who must enter pass codes or use other authentication means to convert the data into readable text, it can provide reasonable assurance that stolen or lost computer equipment will not result in personal data being compromised, as occurred in the recent incident at VA. A decision about whether to use encryption would logically be made as an element of the PIA process and an agency's broader information security program.

While these suggestions do not amount to a complete prescription for protecting personal data, they are key elements of an agency's strategy for reducing the risks that could lead to identity theft.

Public Notification of Data Breaches Has Clear Benefits as Well as Challenges

In the event a data breach does occur, agencies must respond quickly in order to minimize the potential harm associated with identity theft. The chairman of the Federal Trade Commission has testified that the Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified.[28] The Federal Trade Commission has also reported that the overall cost of an incident of identity theft, as well as the harm to the victims, is significantly smaller if the misuse of the victim's personal information is discovered quickly.[29]

Applicable laws such as the Privacy Act currently do not require agencies to notify individuals of security breaches involving their personal information; however, doing so allows those affected the opportunity to take steps to protect themselves against the dangers

[28] Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10.

[29] Synovate, *Federal Trade Commission Identity Theft Survey Report* (McLean, Va.: September 2003).

of identity theft. For example, California's data breach notification law is credited with bringing to the public's notice large data breaches within the private sector, such as those involving ChoicePoint and LexisNexis last year. Arguably, the California law may have mitigated the risk of identity theft to affected individuals by keeping them informed about data breaches and thus enabling them to take steps such as contacting credit bureaus to have fraud alerts placed on their credit files, obtaining copies of their credit reports, scrutinizing their monthly financial account statements, and taking other steps to protect themselves.

Breach notification is also important in that it can help an organization address key privacy rights of individuals, in accordance with the fair information practices mentioned earlier. Breach notification is one way that organizations—either in the private sector or the government—can follow the *openness* principle and meet their responsibility for keeping the public informed of how their personal information is being used and who has access to it. Equally important, notification is consistent with the principle that those controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of the other principles, such as use limitation and security safeguards. Public disclosure of data breaches is a key step in ensuring that organizations are held accountable for the protection of personal information.

Concerns Have Been Raised About the Criteria for Issuing Notices to the Public

Although the principle of notifying affected individuals (or the public) about data breaches has clear benefits, determining the specifics of when and how an agency should issue such notifications presents challenges, particularly in determining the specific criteria for incidents that merit notification. In congressional testimony, the Federal Trade Commission[30] raised concerns about the threshold at which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects. First,

[30] Federal Trade Commission, *Prepared Statement on Data Breaches and Identity Theft*, p. 10.

notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion. Second, a surfeit of notices, resulting from notification criteria that are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant. Finally, the costs to both individuals and business are not insignificant and may be worth considering. FTC points out that, in response to a security breach notification, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on credit files, or obtain a new driver's license number. These actions could be time-consuming for the individual and costly for the companies involved. Given these potential negative effects, care is clearly needed in defining appropriate criteria for required breach notifications.

While care needs to be taken to avoid requiring agencies to notify the public of trivial security incidents, concerns have also been raised about setting criteria that are too open-ended or that rely too heavily on the discretion of the affected organization. Some public advocacy groups have cautioned that notification criteria that are too weak would give companies an incentive not to disclose potentially harmful breaches, and the same concern would apply to federal agencies. In congressional testimony last year, the executive director of the Center for Democracy and Technology argued that if an entity is not certain whether a breach warrants notification, it should be able to consult with the Federal Trade Commission.[31] He went on to suggest that a two-tiered system may be desirable, with notice to the Federal Trade Commission of all breaches of personal data and notice to consumers where there is a potential risk of identity theft. The Center for Democracy and Technology's comments regarding the Federal Trade Commission were aimed at commercial entities such as information resellers. A different entity—such as OMB, which is responsible for overseeing security and privacy within the federal government—might be more

[31] Center for Democracy and Technology, *Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Government Use* (Washington, D.C.: Apr. 13, 2005), p. 7.

appropriate to take on a parallel role with respect to federal agencies.

Effective Notices Should Provide Useful Information and Be Easy to Understand

Once a determination has been made that a public notice is to be issued, care must be taken to ensure that it does its job effectively. Designing useful, easy-to-understand notices has been cited as a challenge in other areas where privacy notices are required by law, such as in the financial industry—where businesses are required by the Gramm-Leach-Bliley Act to send notices to consumers about their privacy practices—and in the federal government, which is required by the Privacy Act to issue public notices in the *Federal Register* about its systems of records containing personal information. For example, as noted during a public workshop hosted by the Department of Homeland Security's Privacy Office, designing easy-to-understand consumer financial privacy notices to meet Gramm-Leach Bliley Act requirements has been challenging. Officials from the FTC and Office of the Comptroller of the Currency described widespread criticism of these notices—that they were unexpected, too long, filled with legalese, and not understandable.

If an agency is to notify people of a data breach, it should do so in such a way that they understand the nature of the threat and what steps need to be taken to protect themselves against identity theft. In connection with its state law requiring security breach notifications, the California Office of Privacy Protection has published recommended practices for designing and issuing security breach notices.[32] The office recommends that such notifications include, among other things,

- a general description of what happened;
- the type of personal information that was involved;
- what steps have been taken to prevent further unauthorized acquisition of personal information;

[32] State of California, *Recommended Practices on Notice of Security Breach.*

- the types of assistance to be provided to individuals, such as a toll-free contact telephone number for additional information and assistance;
- information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies; and
- information on where individuals can obtain additional information on protection against identity theft, such as the Federal Trade Commission's Identity Theft Web site (www.consumer.gov/idtheft).

The California Office of Privacy Protection also recommends making notices clear, conspicuous, and helpful by using clear, simple language and avoiding jargon, and it suggests avoiding using a standardized format to mitigate the risk that the public will become complacent about the process.

The Federal Trade Commission has issued guidance to businesses on notifying individuals of data breaches that reiterates several key elements of effective notification—describing clearly what is known about the data compromise, explaining what responses may be appropriate for the type of information taken, and providing information and contacts regarding identity theft in general. The Commission also suggests providing contact information for the law enforcement officer working on the case, as well as encouraging individuals who discover that their information has been misused to file a complaint with the Commission.[33]

Both the state of California and the Federal Trade Commission recommend consulting with cognizant law-enforcement officers about an incident before issuing notices to the public. In some cases, early notification or disclosure of certain facts about an incident could hamper a law enforcement investigation. For example, an otherwise unknowing thief could learn of the potential value of data stored on a laptop computer that was originally stolen purely for the value of the hardware. Thus it is recommended that

[33] Federal Trade Commission, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* (Washington, D.C.: June 2004).

organizations consult with law enforcement regarding the timing and content of notifications. However, law enforcement investigations should not necessarily result in lengthy delays in notification. California's guidance states that it should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

When providing notifications to the public, organizations should consider how to ensure that these are easily understood. Various techniques have been suggested to promote comprehension, including the concept of "layering."[34] Layering involves providing only the most important summary facts up front—often in a graphical format—followed by one or more lengthier, more narrative versions in order to ensure that all information is communicated that needs to be. Multilayering may be an option to achieving an easy-to-understand notice that is still complete. Similarly, providing context to the notice (explaining to consumers why they are receiving the notice and what to do with it) has been found to promote comprehension,[35] as did visual design elements such as a tabular format, large and legible fonts, appropriate white space, and simple headings.

Although these techniques were developed for other kinds of notices, they can be applied to those informing the public of data breaches. For example, a multilayered security breach notice could include a brief description of the nature of the security breach, the potential threat to victims of the incident, and measures to be taken to protect against identity theft. The notice could provide additional details about the incident as an attachment or by providing links to additional information. This would accomplish the purpose of communicating the key details in a brief format, while still providing

[34] This concept was discussed during a recent public workshop on "Transparency and Accountability: The Use of Personal Information within the Government," hosted by the DHS Privacy Office.

[35] At the DHS workshop, panelists from the Federal Trade Commission and the Office of the Comptroller of the Currency presented these findings of an interagency research project on design of easy-to-understand consumer financial privacy notices. Kleimann Communication Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project* (Feb. 28, 2006).

complete information to those who require it. Given that people may be adversely affected by a compromise of their personal information, it is critical that they fully understand the nature of the threat and the options they have to address it.

In summary, the recent security breach at VA has highlighted the importance of implementing effective information security practices. Long-standing information security control weaknesses at VA have placed its information systems and information, including personally identifiable information, at increased risk of misuse and unauthorized disclosure. Although VA has taken steps to mitigate previously reported weaknesses, it has not implemented a comprehensive, integrated information security program, which it needs in order to effectively manage risks on an ongoing basis. Much work remains to be done. Only through strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight can VA address its persistent, long-standing control weaknesses.

To reduce the likelihood of experiencing such breaches, agencies can take a number of actions that can help guard against the possibility that databases of personally identifiable information are inadvertently compromised: strategically, they should ensure that a robust information security program is in place and that PIAs are developed. More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting data retention, limiting access to personal information and training personnel accordingly, and considering using technological controls such as encryption when data need to be stored on mobile devices.

Nevertheless, data breaches can still occur at any time, and when they do, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. Care is needed in defining appropriate criteria if agencies are to be required to report security breaches to the public. Further, care is also needed to ensure that notices are useful and easy to understand, so

that they are effective in alerting individuals to actions they may want to take to minimize the risk of identity theft.

We have previously testified that as Congress considers legislation requiring agencies to notify individuals or the public about security breaches, it should ensure that specific criteria are defined for incidents that merit public notification. It may want to consider creating a two-tier reporting requirement, in which all security breaches are reported to OMB, and affected individuals are notified only of incidents involving significant risk. Further, Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to the public.

Messers. Chairmen, this concludes our testimony today. We would be happy to answer any questions you or other members of the committee may have.

Contacts and Acknowledgments

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, koontzl@gao.gov, or Gregory Wilshusen, Director, Information Security, at (202) 512-6244, wilshuseng@gao.gov. Other individuals who made key contributions include Idris Adjerid, Barbara Collier, William Cook, John de Ferrari, Valerie Hopkins, Suzanne Lightman, Barbara Oliver, David Plocher, Jamie Pressman, J. Michael Resser, and Charles Vrabel.

Attachment 1: Selected GAO Products

Products Related to VA Information Security

Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-98-175. Washington, D.C.: September 23, 1998.

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls. GAO/AIMD-99-161. Washington, D.C.: June 8, 1999.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. GAO/AIMD-00-5. Washington, D.C.: October 4, 1999.

VA Systems Security: Information System Controls at the North Texas Health Care System. GAO/AIMD-00-52R. Washington, D.C.: February 1, 2000.

VA Systems Security: Information System Controls at the New Mexico VA Health Care System. GAO/AIMD-00-88R. Washington, D.C.: March 24, 2000.

VA Systems Security: Information System Controls at the VA Maryland Health Care System. GAO/AIMD-117R. Washington, D.C.: April 19, 2000.

Information Technology: Update on VA Actions to Implement Critical Reforms. GAO/T-AIMD-00-74. Washington, D.C.: May 11, 2000.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. GAO/AIMD-00-232. Washington, D.C.: September 8, 2000.

Major Management Challenges and Program Risks: Department of Veterans Affairs. GAO-01-255. Washington, D.C.: January 2001.

VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist. GAO-01-550T. Washington, D.C.: April 4, 2001.

VA Information Technology: Progress Made, but Continued Management Attention is Key to Achieving Results. GAO-02-369T. Washington, D.C.: March 13, 2002.

Veterans Affairs: Subcommittee Post-Hearing Questions Concerning the Department's Management of Information Technology. GAO-02-561R. Washington, D.C.: April 5, 2002.

Veterans Affairs: Sustained Management Attention is Key to Achieving Information Technology Results. GAO-02-703. Washington, D.C.: June 12, 2002.

VA Information Technology: Management Making Important Progress in Addressing Key Challenges. GAO-02-1054T. Washington, D.C.: September 26, 2002.

Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements. GAO-05-552. Washington, D.C.: July 15, 2005.

Products Related to Privacy Issues

Privacy: Key Challenges Facing Federal Agencies. GAO-06-777T. Washington, D.C.: May 17, 2006.

Personal Information: Agencies and Resellers Vary in Providing Privacy Protections. GAO-06-609T. Washington, D.C.: April 4, 2006.

Personal Information: Agency and Reseller Adherence to Key Privacy Principles. GAO-06-421. Washington, D.C.: April 4, 2006.

Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain. GAO-05-866. Washington, D.C.: August 15, 2005.

Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure

Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public. GAO-05-864R. Washington, D.C.: July 22, 2005.

Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights are Under Way. GAO-05-710. Washington, D.C.: June 30, 2005.

Electronic Government: Federal Agencies Have Made Progress Implementing the E-Government Act of 2002. GAO-05-12. Washington, D.C.: December 10, 2004.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges, GAO-04-823. Washington, D.C.: July 21, 2004.

Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548. Washington, D.C.: May 4, 2004.

Privacy Act: OMB Leadership Needed to Improve Agency Compliance. GAO-03-304. Washington, D.C.: June 30, 2003.

Data Mining: Results and Challenges for Government Programs, Audits, and Investigations. GAO-03-591T. Washington, D.C.: March 25, 2003.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

Information Management: Selected Agencies' Handling of Personal Information. GAO-02-1058. Washington, D.C.: September 30, 2002.

Identity Theft: Greater Awareness and Use of Existing Data Are Needed. GAO-02-766. Washington, D.C.: June 28, 2002.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

Attachment 2. Chronology of Information Security Weaknesses Identified by GAO

Year	GAO report	VA location or agency	Information security control areas: Access control	Physical security	Segregation of duties	Change control	Service continuity	Security program
1998	GAO/AIMD-98-175	Austin	●	●	●	●	●	●
		Dallas	●	●			●	●
		Albuquerque	●	●	●		●	●
		Hines	●	■	■	■	■	●
		Philadelphia	●	■	■	■	■	●
1999	GAO/AIMD-99-161	Austin	●			●		●
2000	GAO/AIMD-00-232	Maryland	●	●	●	●	●	●
		New Mexico	●	●	●	●	●	●
		North Texas/Dallas	●	●	●		●	●
2000	GAO/AIMD-00-5	VA	●		●			●
2002	GAO-02-703	VA	■	■	■	■	■	●
2005	GAO-05-552	VA	●	■	●	●	●	●

● Weakness found in this area

■ Control area not included in scope of audit

Source: GAO reports.

Notes: Hines is a suburb of Chicago.

Full citations are provided in attachment 1.

DEPARTMENT OF VETERANS AFFAIRS
Veterans Benefits Administration
Washington, D.C. 20420

May 10, 2006

VBA Letter 20-06-35

Director (00)

All VA Regional Offices and Centers

SUBJ: VBA Oversight and Accountability—OIG CAP Report Findings

Purpose

This letter reinforces VBA's commitment to ensuring appropriate oversight and accountability for benefits administration and financial and management controls.

Background

On March 31, 2006, the Office of Inspector General (OIG) issued the Summary Report of Combined Assessment Program (CAP) Reviews at VBA regional offices during the period of October 2004 through September 2005. All VBA services, staff offices, and regional offices receive OIG reports electronically from the VAOIG Reports Staff. These reports can also be found on the Program Integrity and Internal Controls Staff intranet site.

FY 2005 OIG CAP Report Findings

The OIG 2005 summary outlined CAP review results from 17 VARO reviews and highlighted 11 areas needing improvement at 2 or more VAROs:

- Benefits Delivery Network Information Management Controls
- Compensation and Pension Benefit Payments to Incarcerated Veterans
- Compensation and Pension Future Examinations
- Compensation and Pension Hospital Adjustments
- Fiduciary and Field Examinations
- Government Purchase Cards
- Information Security
- Large Retroactive Payment Controls
- Management Performance
- Security of Sensitive Records
- Vocational Rehabilitation and Employment

Directors (00)

A summary of the OIG 2005 findings and recommendations for each of the operational activities reviewed is enclosed.

FY 2006 OIG CAP Report Findings

Although OIG suspended CAP reviews of VBA regional offices effective February 1, 2006, OIG issued eight CAP reports this fiscal year. Analysis of these reports identified recurring findings needing improvement in the following areas:

- Government Purchase Cards
- Benefits Delivery Network Security
- Benefits Delivery Network System Generated Messages
- Compensation and Pension Hospital Adjustments
- Compensation and Pension Benefit Payments to Incarcerated Veterans
- Fiduciary and Field Examinations

Regional office directors should review these findings in light of your existing internal controls and systematic analyses of operations to ensure appropriate oversight is in place to identify and correct any problems at your offices. Appropriate internal controls must be established and monitored on a regular basis to protect the integrity of our benefit delivery processes and systems. While authority for establishing and monitoring these controls is often delegated to those with functional responsibility, you are ultimately accountable for compliance.

Questions

If you have questions, please contact your assigned Office of Field Operations analyst or Kurt Hessling, Director of the Program Integrity and Internal Controls Staff at (202)-273-7593.

/s/

Daniel L. Cooper
Acting Under Secretary for Benefits

Enclosure

Enclosure

Summary Report of CAP Reviews at VBA Regional Offices October 2004 through September 2005

Findings and recommendations for each of the operational activities reviewed are summarized below.

Benefits Delivery Network Information Management Controls

Benefits Delivery Network (BDN) information management controls needed improvements at 6 of 17 VAROs. Results showed that BDN system-generated messages were not processed timely or properly, which resulted in overpayments and underpayments of veterans' benefits. To improve controls, the following recommendations were made:

- Process BDN system messages in a timely manner.
- Take corrective actions as needed for inappropriate benefit payments, including overpayments and underpayments.

Compensation and Pension Benefit Payments to Incarcerated Veterans

Controls over benefit payments to incarcerated veterans needed improvement at 5 of 15 VAROs. The CAP reviews identified benefit processing deficiencies and overpayments that occurred because reviews of information were not completed in a timely manner. To improve operations, the following recommendations were made:

- Ensure timely processing of benefit adjustments, and follow up when necessary to determine incarcerated veterans' status and reduce payments.
- Ensure prompt reviews of information that affects benefit payments to incarcerated veterans.

Compensation and Pension Future Examinations

Improved controls for future compensation and pension (C&P) examinations were needed at two of two VAROs. The staff did not ensure that required examinations were scheduled and conducted, and award adjustments were not processed when appropriate. To improve controls, the following recommendations were made:

- Ensure award adjustments are made and that future examination dates are input into BDN.
- Provide refresher training to rating specialists to emphasize the importance of reviewing veterans' disabilities subject to reduction.

Compensation and Pension Hospital Adjustments

C&P benefits for veterans hospitalized for extended time periods at Government expense were not reduced as required at any of the 17 VAROs. Results showed that: (1) Veterans Service Center (VSC) staff did not always identify hospitalized veterans whose benefits needed adjusting, (2) C&P benefits to hospitalized veterans were not reduced as required and some overpayments were not collected, (3) VSC needed to review Automated Medical Information Exchange (AMIE) admission reports and consult with medical center staff to ensure compliance with notification requirements for hospitalized veterans, and (4) VAROs needed to provide refresher training for VSC staff. To improve operations, the following recommendations were made:

- Provide VSC staff training that emphasizes the importance of reviewing medical records in claims folders to identify cases requiring benefit adjustments.

- Ensure prompt, appropriate actions to adjust benefit payments to veterans hospitalized at Government expense for a period of 90 days or more, and initiate collection actions when necessary.

- Require review of AMIE reports and identification of hospitalized veterans whose C&P awards require adjustment, and forward AMIE reports to the appropriate VA Pension Maintenance Centers or VAROs of jurisdiction.

- Take actions to revise the Systemic Analyses of Operations program to require that VARO staff conduct a 100-percent review of VA health care facility listings of hospitalized veterans, rather than samples of veterans on the listings.

Fiduciary and Field Examinations

Improvements were needed in fiduciary and field examination (F&FE) activities at 8 of 13 VAROs. Accountings were not always accurate or completed in a timely manner. Management needed to improve the oversight of incompetent veterans by ensuring accountings and field examinations were conducted when needed, and that appropriate corrective actions were taken to address program deficiencies. To improve operations, the following recommendations were made:

- Ensure that F&FE staff perform initial appointments and complete field examinations and accountings accurately and within required timeframes.

- Institute appropriate controls to ensure timely actions are taken when inappropriate investments are identified.

- Require F&FE staff to follow up on delinquent fiduciary accountings and, when required, refer delinquent accountings to field examiners, the OIG, or the VA Regional Counsel.

- Ensure F&FE staff establish proper controls to obtain bonds when required, provide refresher training on bonding requirements, and direct F&FE staff to obtain bonds or document reasons for not obtaining bonds.

Government Purchase Cards

The OIG's report Major Management Challenges Fiscal Year 2005 (Report Number 06-00480-26, November 15, 2005), identified the Government purchase card program as a serious VA management problem. CAP reviews found various purchase card deficiencies at 10 of 15 VAROs, including: insufficient supporting documentation, problems with reconciliations and certifications, single purchase limits that were not enforced, use of cards by unauthorized individuals, split purchases, not using established national contracts, a lack of training, and inadequate separation of duties between billing officers and purchase card coordinators. To improve operations, the following recommendations were made:

- Monitor and control activities at individual VAROs to ensure that requirements are followed and documentation is appropriate for purchase card use, approvals, purchases, billing statements, reconciliations, and other activities.

- Ensure that initial and refresher training for cardholders and approving officials is provided and documented.

- Ensure that purchase limit thresholds are enforced, and that warrants are established for cardholders with single purchase limits in excess of $2,500.

Information Security

The Major Management Challenges Fiscal Year 2005 report identified information security as a serious VA management problem. CAP reviews found that information security needed improvement at 7 of 15 VAROs. The vulnerabilities could lead to misuse or loss of sensitive information and data. Areas for improvement included access control, contingency planning, and physical security of information technology equipment. To improve operations, the following recommendations were made:

- Develop contingency plans and obtain certification and accreditation of automated information systems.1

- Enhance physical security and environmental controls for computer rooms and equipment.

- Ensure that Information Security Officers routinely test security controls.

[Areas where improvement is needed as outlined in the CAP reports include strong password verification required to gain access to the automated information system

1 The VA Secretary issued a memorandum dated November 19, 2004, requiring every VA system to be successfully certified and accredited no later than August 31, 2005.

(AIS); identify an off-site storage facility in the AIS contingency plan; IT equipment inventory needs to be included in the IT contingency plan; limit user access to hours necessary to perform assigned duties; obtain accreditation and certification of AIS; upgrade security and environmental controls for computer rooms; improve contingency plan to designate alternate processing site to provide backup service in an emergency; and store backup tapes in a secure location].

Large Retroactive Payment Controls

Controls for retroactive C&P benefit payments of $25,000 or more needed improvement at 3 of 17 VAROs. Verification of retroactive payments were not timely, not performed, not documented, or were not signed by employees with third-party signature authority, resulting in overpayments and underpayments of veterans' benefits. To improve operations, the following recommendations were made:

- Improve controls to ensure that retroactive payments of $25,000 or more receive a supervisory third-party review and timely verification review, ensure the accuracy of award payments, and pursue recovery of overpayments.

- Ensure that staff receive refresher training on retroactive payment requirements.

Management Performance

Management at three of four VAROs needed to improve performance in selected activities to meet national VBA performance goals, including reduction of the inventory of pending rating claims and the timeliness and accuracy of workload accomplishment. To improve operations, the following recommendation was made:

- Continue to monitor timeliness of rating actions and fiduciary activities to meet VBA's nationwide performance goals.

[Specific areas for improvement as outlined in the CAP reports include management's attention to pending non-rating actions; fiduciary initial appointments and field exams; average rating pending time, fiduciary accuracy, notices of disagreement; VR&E rehabilitation rate compared to the national goal; and reducing the inventory of pending rating claims].

Security of Sensitive Records

Security of sensitive records needed improvement at 8 of 17 VAROs. Required reviews of the security of hardcopy and electronic files were not performed, access to file cabinets containing employee-veteran claims folders and other sensitive records was not properly controlled, sensitive files were not secured in locked filing cabinets, files were not maintained at designated VAROs of jurisdiction, and sensitive electronic records were not secured through the Common Security User Manager application. To improve security of sensitive records, the following recommendations were made:

- Ensure that hard copy sensitive records are kept in locked file cabinets, and electronic records are secured through the Common Security User Manager application.

- Limit access to keys for locked claims folders to authorized staff, and use a centralized log system to control and monitor access to the files.

- Conduct audits of sensitive files to ensure that they are securely maintained at the proper locations, and that the locked files include appropriate files.

Vocational Rehabilitation and Employment

Improvements in Vocational Rehabilitation and Employment (VR&E) activities were needed at 9 of 13 VAROs. Areas for improvement included claims processing; timeliness of services; needs assessments; documentation; data entry; and monitoring, control, and management of VR&E cases. To improve program activities, the following recommendations were made:

- Ensure that VR&E staff complete and document needs assessments and rehabilitation plans.

- Strengthen case management, including timeliness and accuracy of work.

- Require that VR&E staff monitor data entry to automated systems for accuracy, manually correct the data as appropriate, and update the veterans' case status in a timely manner.

[Specific areas for improvement as outlined in the CAP reports include timeliness of service; file documentation; and accuracy of data and decisions].

Appendix E
SAMPLE RULES OF BEHAVIOR

(DISCLAIMER – Any policy, procedural, or job description published or sponsored by the VAOCIS takes precedence over the contents of Appendix B. The guidance herein is for our use until superceded by VA.)

The following is a sample of a VBA field facility Rules of Behavior document. The document would be retained by the user, with the final page (signatures) removed and returned to the ISO.

These Rules of Behavior apply to all users of Veterans Affairs (VA) information technology (IT) systems.

1.1 Basic Orientation

1.11 Why Security Is Important For Everyone

All users of VA IT resources should be aware that any system potentially contains valuable and sometimes sensitive government and/or personal information, which must be protected to prevent disclosure, unauthorized changes, and loss. Each part of a system can introduce vulnerabilities to the whole, so protection must be consistent in order to be effective. On a larger scale, since VA IT resources are typically connected to VA and other sensitive government networks (e.g., Social Security Administration, Internal Revenue Service, Department of Defense), any system compromise is a potential threat on a grand scale to the Federal Government.

1.12 User Information and Contacts

This Information will be provided in a separate enclosure.

1.20 The VA IT Environment

1.21 General Information

a. All VA IT users must read and abide by these Rules of Behavior.

b. Users will process only data that pertains to official business. However, workstations may be used for limited personal use (i.e. reading on-line newspapers, checking bank accounts) as long as this use does not incur any cost to the government, does not violate any laws, regulation or standards, local VA or VBA policies, and the activity takes place during personal time (i.e., lunch time or after hours).

1.22 Sensitive Data Considerations

a. Unclassified but sensitive information on VA IT resources should be protected as For Official Use Only (FOUO). The following categories are examples of information that is normally FOUO:

b. Personal information subject to the Privacy Act of 1974, including Social Security number and benefits information.

c. Reports that disclose security vulnerabilities.

d. Information that could result in physical risk to individuals.

e. All output that contains FOUO information should be so marked or labeled by the user who generated the material, and then stored or transmitted with appropriate protection. The designation "For Official Use Only" should be marked, stamped or permanently affixed to the top and bottom of the outside of the front and back covers (if any), on the title page and on all pages of documents or information requiring such control. All diskettes or other magnetic media containing sensitive information should be similarly labeled and stored in locked containers (e.g., desks, filing cabinets, etc.).

f. Sensitive documents that are no longer needed should be shredded.

g. Magnetic media (e.g., diskettes and hard drives) that have been used for sensitive information may contain information even after the files are deleted. The information may be recoverable, even if a normal directory listing of the medium says it is empty. Before discarding magnetic media, users should do one of the following:

1. Degauss (erase all magnetic patterns on) the media.

2. Destroy the magnetic medium physically (open the plastic floppy disk casing, remove the disk, and shred it).

3. Use an approved software program to completely delete all files on the medium and overwrite them with ones and zeroes.

b. If you need assistance in disposing of magnetic media, consult your System Administrator or Information Systems Security Officer.

1.30 Passwords

a. Do not record your password in writing.

b. Do not share your password or accept another user's password if offered. Sharing passwords defeats the system's user identification and authentication mechanisms. In addition to sharing access privileges, participants share liability for any unauthorized behavior traced to the shared User ID and password.

c. Passwords will be a minimum of eight but not more than 15 characters in length.

d. Your password should be something you can easily remember.

c. Your password should not be something that another can guess so, do not use the name of your spouse, pets, or children, or words found in a dictionary. Single-word passwords are susceptible to being guessed by software routines that check every word in the dictionary.

f. Use two small groups of alphabetical or numeric characters, or words, linked by a number or typographical character (&, *, !, etc.).

g. SAs have no way to look up your password. If you forget it, your SA will change it and make you pick a new password.

h. The system will prompt you will change your password every 90 days.

i. A new password cannot be one you used recently. Certain operating systems (i.e., Windows NT) remember as far back as the ten most recently used passwords.

j. If there is a reason, you may change your password before the end of 90 days, but only after three days have elapsed since the password to be changed was created. If there is a compelling reason to change the existing password before the end of the three-day period (such as a suspected compromise) contact the SA.

k. Users will be locked out of the system after six consecutive incorrect password entries and will be required to contact the SA.

l. Passwords are case sensitive. Users should not attempt to enter a password with the "caps lock" key enabled.

1.40 Electronic Mail

a. Government-provided electronic mail is intended for official and authorized purposes only. Electronic mail users must exercise common sense, good judgment, and propriety in the use of Government resources. While short personal messages are acceptable, parallel to the way Government telephones are sometimes used, other non-official uses are prohibited. Personal messages sent to groups of people are likely to fall into the category of prohibited use. Therefore, personal messages should not be sent to large groups. The presumption is that no notice except those sent by VA systems administrators or support personnel is so important that it should be broadcast globally to everyone within an organization or VA-wide without the approval of the appropriate office head. Broadcast messages are those sent to public groups listed (i.e., VBA, VHA, NCA, etc.) in the email software's address book or large personal groups.

b. Well intentioned notices including: retirements, deaths, births, lost or found property, or car lights left on, are not appropriate material for broadcast messages.

c. Employees are prohibited from using VA office automation or electronic mail systems to distribute information on any non-Government activities, including but not limited to: charitable events, religious observances, fund-raiser, and personal business. Employees who misuse Government resources in this way may have electronic mail privileges withdrawn and may be subject to disciplinary action.

Government employees should have no expectation of privacy when using the VA mail system. Electronic mail is not confidential. SAs may read the electronic mail of others (for a specific purpose) with appropriate authorization. In addition, technical or administrative problems may create a situation in which it is necessary for an administrator or system manager to read message text. Moreover, VA views electronic mail messages to be Government property, and officials may have access to those messages whenever there is a legitimate Government purpose for such access. Users should treat the electronic mail system like the use of Government-provided inter-office mail system.

d. Do not use government email to send personal or official email to your home, friends, or other recipients outside the VBA network that contains sensitive data, e.g. SSNs, personal addresses, etc. Data sent outside VA over the public network is protected.

1.50 Internet Use

It is VA policy to safeguard VA data and reduce unnecessary risks to the integrity, availability, and confidentiality of VA computer and communication resources that may arise because of Internet abuse and misuse. This policy governs the activities of VA Internet users, but does not address Internet security.

1.51 General Policy

a. VA information systems will be used for only official Internet use and authorized personal Internet use. Official Internet use means that VA information systems may be used to access Internet resources for official communication, research, or professional development, as long as this access relates to the VA mission. Authorized personal Internet use means that with the permission of the VA, Internet resources may be accessed for authorized personal use either before or after work hours, during lunch periods, or during other authorized breaks during the day.

b. Authorized personal use applies to all government personnel and, at the discretion of the VA, may be extended to contractor personnel working in VA facilities.

c. In no case will the personal use of government resources be allowed to interfere with the VA mission, pose a hazard to the security of government data or resources, or reflect adversely on the VA or the Federal Government. The VA may revoke the privilege of authorized personal use at any time for any perceived misuse of government resources.

1.52 Prohibited Internet Uses

The following are prohibited uses of the Internet:

d. Possessing or distributing child pornography is a federal crime. Anyone caught with child pornography on a government computer will be prosecuted. VA does not recognize any legitimate reason for the use of pornography of any sort. Accessing any pornographic site is considered fraud, waste, and abuse of government resources and will be reported to the local network support and ISO.

b. Accessing, transmitting, storing, or distributing offensive material (e.g., racist literature, material, or symbols).

c. Participating in "chat room" discussions that are not for official business.

d. Accessing known "hacker" sites and downloading hacking tools without special authorization.

e. Lobbying or advocacy on behalf of any political organization or religious group not affiliated with the VA.

f. Viewing, damaging, deleting, or interfering with the functioning of any system or any other person's files or communications.

g. Conducting Internet activities for personal or commercial financial gain, along with unauthorized fund-raising. Fund-raising for certain government-approved organizations may be authorized by VA.

h. Attempting to circumvent or disable any Internet security or auditing system without prior authorization from the ISO or SA. This includes disabling virus detection mechanisms and modifying or altering the operating system of the hardware used to connect to the Internet.

i. Downloading, installing, storing, or using the software from the Internet in violation of any patent, copyright, or license agreements is prohibited. All files downloaded from the Internet must be scanned using approved antivirus software before they are opened, executed, or forwarded to other users.

1.53 Transmission of Data Over the Internet

Transmission of data over the Internet requires the use of appropriate safeguards. Sensitive and "FOUO" information must not be transmitted over the Internet unless appropriate safeguards (e.g., encryption) have been implemented. Since these safeguards are not available to VBA end-users, transmission of sensitive and "FOUO" information outside the VA's Wide-Area Network (i.e. via Internet) is prohibited.

1.54 Multiple User Computer Systems Used for Internet Access

Not applicable

1.55 Dial-Up Access to the Internet Using a Modem

Dial-up access to the Internet is prohibited for users connected to the VA information systems.

1.60 Web Page Establishment and Maintenance

Not applicable

1.70 Interacting With Administrators

a. Occasionally, users need to call upon administrators at various levels in order to obtain services or meet requirements for a specific task. Some routine occasions are listed below.

b. When you start a new job, or your job description changes, coordinate your VA IS access requirements and parameters with your first line supervisor.

c. When you need to obtain membership in a shared directory, or change or terminate your membership privileges, see the owner of that directory.

d. When you need other access privileges in order to do your job, notify your supervisor.

e. When you find that your access to VA resources is beyond what you need to do your job, notify your supervisor.

f. When you need to remove any computer resource from VA premises, see your supervisor for approval and a hand receipt. Resources may only be removed from VA premises for official use.

1.80 Configuration Management

1.81 Things You May Change

You may change the Windows "wallpaper" background (using one of the standard, system-provided backgrounds).

1.82 Things You May Not Change

a. Do not install any software onto your workstation or any other VA system resources. Only the VA SA (or his/her designated representative) is authorized to load software on workstations or servers.

b. Do not attempt to add printers to the ones your workstation can select. If you need access to another printer, see your supervisor or SA. Normally, users will be assigned to the printer nearest to their workstation area.

c. Do not add any additional hardware or peripheral devices to any workstation, server or other system resource. This includes all devices such as extra memory, hard drives, printers, scanners, additional servers, additional processors, etc. These tasks are handled by the SA and subject to configuration control.

1.90 Unauthorized Activities

All VA IT system users are held strictly accountable for their actions while on the system. User activity may be monitored and system activity audited to detect unauthorized behavior. Unauthorized activity may result in a warning, reprimand, loss of access, formal disciplinary action (including dismissal), or even legal action (such as a fine or imprisonment).

Unauthorized activities include:

a. Entering unauthorized, inaccurate, or false information. Do not delete or manipulate information inappropriately.

b. Using data for which you have not been granted authorization. Do not explore data or IS capabilities that are not related to your job or attempt to access information which you do not have authority to access. If you have any questions about the limits of your authorization, consult your supervisor for clarification.

c. Retrieving information for someone who does not have access to it himself/herself, except as specifically authorized:

1. In your job description.

2. By your supervisor.

d. Violating copyright and site licenses of proprietary software. This may happen when multiple copies of licensed software is installed, as well as when unlicensed software is installed.

e. Installing unauthorized software. Do not install outside software (including other agency software, shareware, freeware, personally purchased, or pirated software) on a VA system.

f. Installing modems (either internal or external) on a workstation, server or any other VA system resource. Although covered in the preceding section on configuration management, modems deserve special attention because they are a well-known way to bypass firewall protection. In particular, modems that are set to answer calls enable system access from outside the facility and may be regarded as a malicious breach of security.

g. Storing or processing classified national security information on a VA system. If, for any reason, classified information is introduced to a VA system, notify your SA as soon as possible.

e. Leaving your computer logged in to the VA network, but unprotected. Log-off your workstation whenever you are away from the immediate work area, unless a screen saver feature with a password enabled is properly invoked.

2.00 Your Role In Protecting the VA IT System Resources

a. Ensure that any data that is visible on the workstation monitor screen cannot be viewed by unauthorized personnel.

b. Invoke an appropriate level of protection whenever you leave your workstation unattended. For short periods, (visiting the restroom, or retrieving output from a printer that is out of sight of your workstation) you may use a password-protected screen saver feature. For longer periods, (going to another floor or leaving the building), log-off the workstation. The following guidelines will be followed when using the screen saver option:

1. Only screen savers provided with the system (e.g., Microsoft Windows) are authorized. No other screen savers are to be installed.

2. The password option for the screen saver must be invoked by the user. The password created will be generated by the user. The criteria for generating that password will be the same as that used for creating a VA network log-on password. The screen saver password must not be the same password used for logging on to other VA networks and systems.

3. The user will ensure that the screen saver activates before leaving the workstation unattended. This must be done, because there are conditions in a session that will delay or preclude the screen saver from activating (the print pop-up is present on the screen, data exchanges are occurring between server and workstations, etc.).

c. Ensure printouts are retrieved as soon as possible. Output should not be left unattended for any longer than is necessary.

d. Protect your equipment (workstation, diskettes, etc.) from physical damage. Ensure that your workstation is clean, ventilated, and located in a place where it is not likely to be bumped or knocked over. Keep food and drinks where they won't get spilled on the equipment.

e. Safeguard VA resources against waste, loss, abuse, unauthorized use, and misappropriation.

e. Scan all disks for viruses before use, especially if they are received from external sources. Discontinue use of any VA IS resources that show indications of being infected by a virus and immediately report any incidents to the ISO.

f. Report any security incidents or suspected security incidents, including computer virus infections, to your ISO. The term "security incident" includes any event that may result in the disclosure of sensitive information to unauthorized individuals, or that results in unauthorized access, modification or destruction of system data, loss of system processing capability, or loss or theft of any computer system media.

g. Challenge any unauthorized personnel in your work area.

2.10 Signature

I have read, understand, and will comply with the Rules of Behavior for users of VA IT systems dated [Date of Document]. I have retained a copy for personal reference.

_____ _____

Signature Date

PLEASE PRINT:

_____

Employee Name

_____

Organizational Element

_____

Organization Telephone Number

Questions for the Record
The Honorable Jeff Miller
Chairman
Subcommittee on Disability Assistance and Memorial Affairs
Joint Hearing with Subcommittee Economic Opportunity
House Committee on Veterans' Affairs

June 20, 2006

Hearing on Veterans Benefits Administration Data Security

Question 1: In both your written and oral testimony, you referred to a "rules-of-behavior" policy which employees are required to sign. Please provide me with a copy of this policy. Additionally, how many employees have violated these rules in the past year, and what disciplinary action was taken?

Response: See **Attachment 1** for sample rules of behavior. The Veterans Benefit Administration (VBA) does not have data available on employees who may have violated these rules in the past year.

Question 2: Since the May 3 security incident, you have required that Privacy Awareness and Cyber Security training, originally slated to be completed by the end of the fiscal year, must now be completed by June 30, 2006. Will fast-tracking the training prevent some from fully learning and understanding the requirements?

Response: Because there is such a high awareness of the data issue within the Department of Veterans Affairs (VA), we believe this is an excellent time to escalate the importance of this training to employees. The training methods of delivery remained the same, regardless of when an employee took the training, therefore no content was lost as a result of speeding up the process. The on-line course took the same amount of time, with the same level of testing built into the module. The satellite broadcast was also scheduled for the required length of time, regardless of when viewed. Therefore, everyone was given full opportunity for learning and understanding the content.

Question 3: Have you had to redirect claims adjudication staff to assist with the call centers in light of the data breach? If so, please explain your justification.

Response: Since the call centers started operations on May 22, 2006, one VBA employee has been assigned to each center on a rotational basis to assist contractors with unusual questions, provide training and guidance to call center agents and monitor incoming calls for quality assurance purposes. All employees assigned have been either central office staff or supervisory staff from regional offices. No employee involved with direct service to veterans or claims adjudication has been assigned to work at any of the call centers.

Question 4: You cited, and I quote, "distractions" as the reason for the delay of VETSNET, originally envisioned to replace the Benefits Delivery Network in the late 1980s. Please provide me with a list of those distractions.

Response: There is no list of "distractions" responsible for delays in completion of Veteran's Service Network (VETSNET). The intention of this statement was to reinforce VBA commitment to delivering on the promise for completing VETSNET and successfully moving the compensation and pension program from our legacy system environment to a claims processing environment more in keeping with today's information technology. VBA believes it is imperative to maintain our focus on successfully completing VETSNET. Maintaining this focus may prevent us from taking on new initiatives today, such as creating a new electronic claims file system, despite the merits of the new, but competing, initiatives.

Question 5: VA's Office of Inspector General has found that a number of VBA systems are running on outdated and undated operating systems which pose a security risk. Is it customary to be running outdated software, or is this a result of funding decisions that diverted money to other priorities with VBA?

Response: All VBA workstations are running the same operating system. The imaging management system (TIMS) workstations are all running Windows 2000 and the PCs are all VBA standard workstations. The scanner problem (i.e., several running Windows 95) was resolved by upgrading to Windows 2000. VBA is finalizing plans to migrate all PCs to Windows XP by January 2007.

VBA works diligently to ensure our end users have state-of-the-art hardware and software at their disposal. However, there are times when funding and resources do not allow us to have cutting edge equipment and software.

Question 6: In the VA Inspector General's 2004 Federal Information Security Management Act made 16 recommendations, some of which could be addressed by VBA. Does your office have the authority to act on those, or do you require concurrence/approval from some other entity within the Department?

Response: VBA works very closely with the VA Office of Cyber and Information Security (OCIS) and implements the department's recommended security technical solutions. As an example, VA acquired standard intrusion detection, patch management and Pest Patrol software. VBA, with OCIS concurrence, purchased licenses for Password Policy Enforcer software to ensure use of strong passwords on our networks.

Questions for the Record
The Honorable John Boozman,
Chairman
Subcommittee Economic Opportunity

Question 1: Is it true that encrypting many of the legacy business line systems will dramatically slow down the processing of data?

Response: Our analysis indicates that encryption can diminish performance by as much as 30 percent.

Question 2: Please provide sample copies of the specific security clauses in VR&E counseling contracts.

Response: Currently under the national acquisition strategy (NAS) contracts, there is a statement to comply with Federal Acquisition Regulation (FAR) 52.239-1 "Privacy or Security Safeguards" as follows:

52.239-1 Privacy or Security Safeguards. (Aug 1996)

(a) The contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

All contractors, however, are required to follow all Federal, State, and local regulations and should also be following the two below mentioned FAR regulations. These regulations are not specifically annotated in the NAS contracts. The Office of Acquisition and Materiel Management and the VR&E Service are in the process of developing a letter amending the current contract to remind all contractors that the Privacy Notification and Security Safeguards that must be followed include the following two regulations:

52.224-1 Privacy Act Notification (Apr 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

52.224-2 Privacy Act (Apr 1984)

(a) The Contractor agrees to –

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(i) The system of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on

individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers of employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c) (1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Local regional office contracts are currently established using VA Form 28-1903, which does not have a privacy and security statement incorporated into the contract. The Vocational Rehabilitation and Employment (VR&E) service will resubmit this form to the Office of Management and Budget (OMB) to be modified to include the privacy and security statements. In the meantime, VR&E officers are authorized and continue to issue local contracts which fall under their current warrant levels, and the VR&E service has arranged to have the VR&E officers send their local contractors the same information that is being released to the NAS contractors on privacy and security safeguards.

Question 3: The IG cited the Imaging Management System (TIMS) used to store education benefits data uses vulnerable and obsolete computers to do the scanning. Have those computers been replaced and, if not, when will they be?

Response: All VBA workstations are running the same operating system. The TIMS workstations are all running Windows 2000 and the PCs are all VBA standard workstations. The scanner problem (i.e., several running Windows 95) was resolved by upgrading to Windows 2000. VBA is finalizing plans to migrate all PCs to Windows XP by January 2007.

Question 4: Please provide the Subcommittee with a chart, including milestones, showing the Department's plan to address each of the 16 vulnerabilities noted by the Inspector General. In addition, please provide a narrative describing the issues and resource requirements for each of the 16.

Response: See table below. Please note that due to the extensive collaboration, data collection, and analysis required; the funding needed to remediate the 16 deficiencies identified by the Office of Inspector General (OIG) has yet to be determined.

Issue	Status	Planned Completion Date
1. Centralize IT Security Operations	**In-Progress.** Information Technology (IT) security operations will be centralized with the IT budget, personnel, and authority and responsibility for IT security being placed under the Chief Information Officer (CIO). CIO approval is needed for the new IT organizational structure before this issue can be closed.	Jan 2007
2. Patch Management Program	**In-Progress.** Testing of a patch management system was successfully completed at two Veterans Integrated Service Networks (VISN) in September 2006. From a centralized location within the VISNs, VISN staff was able to inventory and verify patches were installed during the test. Additional testing to be completed includes merging two VISNs by March 2007 and a region of five VISNs by April 2008. After assessing the results, upper VA management will make a decision on whether or not to deploy the system to the rest of VA, including VBA and the National Cemetery Administration (NCA).	Dec 2009
3. Unauthor-ized access and Misuse of Sensitive Data	**In-Progress.** In addition to issuing policies regarding access to and protection of sensitive VA data, VA has developed a plan to address these vulnerabilities. With the CIO's new authority and control over the IT budget, the CIO will now be able to direct remediation of these issues.	Jul 2007
4. Proper Data Classifi-cations in Position Descriptions	**In-Progress.** VA administrations and staff offices, in consultation with the CIO and Office of Human Resources, are undertaking a complete review of position sensitivity/risk level designations and existing background investigation levels for all employees, volunteers, interns, students, residents, and contractors. By November 30, 2006, all administrations and staff offices completed the review of position sensitivity/risk level designations and establish commensurate background investigation requirements. Senior executives will ensure the update of official personnel folders and amendment and revision of contracts, as necessary. Where needed, new background investigations will be initiated as soon as possible.	Jan 2007
5. Obtain timely and complete background investigations	**In-Progress.** An concerted effort is underway to improve VA's performance regarding background investigations with special emphasis on those positions requiring extensive access to sensitive information and computer systems/ networks. Specific activities are cited in response to issue 4 above.	Dec 2007

Issue	Status	Planned Completion Date
6. Intrusion Detection Systems	**In-Progress.** VA has deployed intrusion prevention systems (IPS) and in 2005 completed an assessment of host-based intrusion prevention systems (HIPS) and network-based intrusion prevention systems (NIPS). The HIPS infrastructure was completed in 2005 with the second phase of the HIPS deployment focusing on the servers which is scheduled to be completed by the end of calendar year 2006. The NIPS have been deployed to all enterprise cyber security infrastructure project (ECSIP) gateways, all approved business partner gateways (BPG), all data centers and 37 of the 38 distribution nodes. The next phase of the project involves locating segments of traffic not covered by the VISN distribution nodes, data centers, and BPGs.	Aug 2007
7. Complete Infrastructure Protection Actions	**In-Progress.** A VA "Critical Infrastructure Protection Plan" is in development. VA has developed a Master COOP plan. VA also participated in a Federally-mandated COOP (Continuity of Operations Plan) exercise (called Forward Challenge) during the week of June 19, 2006. VA Directive and Handbook 0320, Comprehensive Emergency Management Program, provides Department-wide policy, responsibilities, procedures, and operational requirements regarding VA's Emergency Management Program.	Jan 2008
8. Data Center Contingency Planning	**In Progress.** The Austin Automation Center (AAC) continues to conduct continuity of operations plan (COOP) tests annually and has worked to integrate their COOP with the resident organizations collocated at their facility. VBA has completed disaster recovery COOP tests with the Information Technology Centers (ITC) and the AAC. plans have been developed to establish a recovery capability for two applications, Virtual VA and TIMS. A benefits delivery network (BDN) disaster recovery exercise was completed in September and October of 2005 between the Hines and Philadelphia ITCs. The annual Hines ITC COOP tabletop scenario exercise was conducted on November 17, 2005.	Aug 2007
9. Certification and Accreditation of Systems	**In Progress.** Although extensive certification and accreditation work was performed in 2005, additional systems exist that may require certification and accreditation. These systems will undergo a certification and accreditation review.	Jan 2007
10. Upgrading/ Terminating External Connections	**In Progress.** NCA shut down its Internet gateway on June 20, 2006 and VBA has a single, certified point of presence serving as the Internet gateway. It is located at the Philadelphia ITC. The Philadelphia ITC has moved to the ECSIP gateway effective February 9, 2006, for all external VBA Internet traffic. Migration of the VISN 21 gateway is 95 percent complete and for VISN 22, only the Loma Linda gateway is still operational and will be shut down by November 17, 2006. The AAC Internet gateway is scheduled to convert to ECSIP by June, 2007, at which time all AAC customers should be migrated to ECSIP.	Jun 2007

Issue	Status	Planned Completion Date
11. Configuration Management	**In-Progress.** All VBA workstations are operating under Windows 2000. All VBA servers are operating under Windows 2003, and implementation plans are underway for workstation upgrades to the Windows XP operating system. No desktop systems or IT servers in the Veterans Health Administration (VHA) use Windows 95 or Windows 98 operating systems. The large majority use the latest operating system, Windows XP. Exceptions include specialized equipment, e.g., medical devices, which are scheduled to be replaced with newer equipment during fiscal 2007. Plans have been developed to upgrade all VA computers to the Windows XP operating system and to upgrade peripheral devices, as necessary, by September 30, 2007.	Sep 2007
12. Movement of VACO Data Center	**In Progress.** The router and switches in the VA Central Office (VACO) computer room are the backbone of the VACO building local area network (LAN), the equipment connecting the VACO building to the other buildings in the VACO campus over the VACO metropolitan area network, and the edge router connecting the VACO building to the VA wide area network (WAN). Plans are to move this equipment to a telecommunications closet on the fifth floor by June 30, 2007, but not later than September 2008. VA has limited capability to complete this faster and will press General Services Administration in this regard.	Sep 2008
13. Application Program/Operating System Change Controls	**In Progress.** VA will develop a national change control policy. This policy is currently in development and will be based on the requirements contained in National Institutes of Standards and Technology (NIST) publications. VA is already required by Federal Information Processing Standards (FIPS) 200, minimum security requirements, to control changes to its information systems. An enterprise change control board will be established by December 31, 2006 to oversee changes to VA systems.	Dec 2007
14. Limiting Physical Access to Computer Rooms	**In Progress.** Better control over physical access through intrusion detection systems has already been achieved in most locations. Information security officers, who are now under the control of the CIO, will have an improved capability to correct these deficiencies. The Secretary's June 28, 2006, Delegation of Authority memorandum, will also significantly enhance the ability of the CIO to ensure that corrective action is taken where proper access controls are needed.	Jan 2007
15. Wireless Devices	**In Progress.** VA acquired a product to mitigate wireless security weaknesses, but it was not kept current throughout VA. The VA Security Operations Center is establishing a wireless penetration and assessment program that will identify and assist the field with remediation of wireless security vulnerabilities. With the IT realignment, the CIO will direct remediation of identified wireless deficiencies. A more extensive review of the wireless security environment needs to occur with remedial action to be completed by September 30, 2007.	Sep 2007

Issue	Status	Planned Completion Date
16. Electronic Transfer of Sensitive Data	**In Progress.** Encryption standards have been developed for VA-controlled laptops, and laptop computers were encrypted using the Guardian solution. In addition, a number of memorandums and directives have been issued regarding protection of VA information. A VA Data Encryption Steering Committee has been established to review the transmission of data over VA networks. It replaces the Transmission of Privacy Information in Clear Text (TOPIC) working group.	Dec 2007

Question 5: Was any data related to the specific information regarding education accounts, voc rehab and employment medical records, or loan guaranty financial data included in the loss?

Response: In their investigation, the Inspector General (IG) reported that a file found on one of the employee's CDs pertained to a project he was working on using vocational rehabilitation data. The employee indicated he did not believe it was on his stolen hard drive because he had no interest in working on that project at home. There is no other indication at this time that education accounts, employment medical records or loan guaranty financial data were included in the loss.

Question 6: Do existing labor agreements contain any provisions for enforcing unauthorized use of access to data? If not, do you anticipate revising labor agreements to enable the Department to hold employees accountable for these types of actions?

Response: VA's existing master labor agreements do not contain provisions for enforcing unauthorized use or access to data. Employees are held accountable for these types of actions even without language negotiated with a labor organization. We do not negotiate standards of conduct in labor agreements because of management's rights and all employees are subject to standards of conduct. Therefore, we do not anticipate revising our labor agreements to hold employees accountable.

Question 7: What arrangements has VA made with Defense Finance Center to protect the active duty, reserve and retiree accounts from unauthorized access? Do you know what DoD is doing to protect those accounts?

Response: VA routinely provides data from the benefits delivery network (BDN) to the Defense Finance and Accounting Service (DFAS) needed to compare payments and reconcile VA/Department of Defense (DoD) pay records. VA currently does not have access to DFAS records.

VA allows limited access to DFAS for processing combat–related special compensation (CRSC) claims. For personnel identified by DFAS as needing access to the BDN, DoD or its contractors must provide VA with information on the employees and their station and submit a certification from their supervisor confirming that access is required. They also fill out a request for access to the local area network. The Assistant Director for Policy in the Compensation and Pension Service is the authorizing official. When DoD

personnel are approved for access, the Information Security Officer (ISO) issues them user passwords and provides them with software that allows them limited access to VA data from DoD computers.

The system is protected in two ways. Compensation and Pension (C&P) service uses the VA virtual private network, which encrypts the data. Also, we have a security agreement with DoD to ensure that its systems have the security in place that VA requires.

C&P Service is not familiar with DoD efforts regarding privacy protection. This question is more appropriately be addressed to DFAS personnel.

Question 8: Did the information lost during this incident include bank account numbers for direct deposit?

Response: The IG report gave no indication that bank account information or direct deposit numbers were included on the stolen hard drive. Since recovery of the stolen equipment, the Federal Bureau of Investigations (FBI) also expressed a high level of confidence that information contained on the hard drive was not compromised.

Question 9: What is the Department doing to lessen its dependence on social security numbers?

Response: Since the early 1970s, social security numbers (SSNs) have been used to track and control veterans' claims records and benefit award payments. To establish a record in the beneficiary identification and records locator system (BIRLS), the veteran's name and at least one other piece of information are necessary. Pursuant to section 5101 (c) of title 38, United States code, any person who applies for or is a receipt of VA compensation or pension benefits is required, upon VA request, to provide his or her SSN to VA and the SSN of any dependent or beneficiary on whose behalf, or based upon whom, such person applies for or is in receipt of such benefit.

Public Law 101-508, The Omnibus Budget Reconciliation Act of 1990, directs VA to match with the Social Security Administration and the Internal Revenue Service for certain veterans receiving total disability compensation benefits based upon a finding of individual unemployability, veterans receiving VA pension benefits, and veterans qualifying for healthcare enrollment based on their income. SSNs are used to perform additional computer matches with other Federal agencies such as DoD, Department of Education, Bureau of Prisons, Office of Personnel Management, and the Railroad Retirement Board.

Computer matches may be initiated based on public law or to fulfill a need demonstrated by VBA or other Federal agency. These matches ensure program integrity by assisting VBA in identifying beneficiaries whose benefits require adjustment or termination based on incarceration; fugitive felon status; underreporting of earned and unearned income; receipt of DoD benefits (e.g., retirement, severance, separation, and drill pay); and return of a veteran (in receipt of disability compensation) to active duty.

SSNs are the key personal identifiers that allow VA and DoD to reconcile eligibility and payment issues for education benefits. These benefits are a combination of VA appropriated funds and/or DoD funds. Therefore, the computer matching agreements between the DoD and VA for the purpose of determining eligibility for education benefits are unique because it allows for both entities to account for expenditures to those deemed eligible by virtue of military service.

Additionally, SSNs are used as key personal identifiers by numerous other Federal agencies and external entities. Therefore, these numbers are needed for VBA to obtain and/or provide information to other external entities. For example,

- To request service medical and personnel records from the Department of Defense and National Personnel Records Center;
- To communicate with schools and training facilities regarding authorization for a veteran to participate in training;
- To prove statutory compliance of funding fee payment;
- To obtain a credit report in the course of underwriting a vendee loan or a Native American Direct Loan (NADL); and
- To receive transmissions from loan servicers regarding a notice of default.

To minimize the unnecessary use of the SSN in VHA systems operations, VHA assigns an Integration Control Number (ICN) as the unique identifier for each patient. This system identifier provides a comprehensive view of a patient's healthcare information without the use of the SSN as the primary identification method. The ICN is a sequentially assigned, non-intelligent number which in itself does not provide any identifying information about a patient. The ICN is not displayed or used by humans to look up information about patients and as system to system identifier it does not provide any information about the patient.

VHA's Health Eligibility Center (HEC) removed the SSN from its enrollment notification/welcome letters over 2 years ago and does not use the SSN on income verification related correspondence. Instead it uses an internal case number. In addition HEC began using barcode technology in lieu of displaying any identifier. This also extends to its internal case number used for income verification activities.

As of December 2006, the volunteer database in VHA will remove the SSN from its applications and data collected.

In VA medical centers and community-based outpatient clinics, VHA has modified its use Veterans Health Information Systems and Technology Architecture (VistA) software so it no longer prints the SSN on its communication mailings, including scheduling reminders and no-show correspondence to veterans. In fiscal year 2004, the SSN was also removed from monthly co-pay billings to veterans.

In other areas such as research, administrative planning, and human resources, the SSN is scrambled, when possible, so the actual SSN is not visible to the naked eye either in electronic form or when printed. In other cased, it is reduced to the last four digits of the number. While these methods do not completely eliminate the use of the SSN, they do reduce the risk of theft or misuse of the number.

For employees, including the many veterans who work for VA, the SSn was removed from the bi-weekly pay statement.

As noted above, VA has taken many steps to eliminate the use of the SSN where it is not mission-critical. However, there are also mandated and legitimate uses for the SSN. In such cases protecting the number is critical. To that end, VA has been working to develop tools, policies, and guidance, to ensue the protection of all personally identifiable information including SSNs. Their steps will maintain a culture where appropriate use of the SSN is protected and all information on our nation's veterans is treated with the highest level of confidentiality.

VA looks forward to working with Congress and other agencies to develop solutions to minimize the use of SSNs. Because of our many data exchanges with DoD, Social Security Administration, Department of Education, Bureau of Prisons, Office of Personnel Management, and the Railroad Retirement Board, to determine entitlements, this will be a challenging task.

Question 10: The constant theme in the testimony presented by the IG and GAO is the need for centralized cyber security, among other things. If VA refuses to adopt a centralized approach to managing its IT systems as required by HR 4061, how can you expect to achieve consistency throughout the VA system on anything related to IT?

Response: The attached memo signed by the Secretary on June 28, 2006, clearly indicates that Cyber Information Security is now centralized under the control and authority of the Assistant Secretary for Information Technology.

Questions for the Record
The Honorable Ginny Brown-Waite

Question 1: If an employee at VA downloads a file, does VA have a system that shows who downloaded that file? If there is a system monitoring this information in place, what does VA do with this data?

Response: VA is a large and diverse agency which uses more than 550 operational IT systems. The legacy systems that VA uses do not have the technological capability to retain information on file downloading by individual users. VA has planned to develop policy governing the reporting requirements of downloading files containing sensitive veteran data. That policy will require staff to report instances of downloading files that contain more than a minimal amount of veteran data.

ATTACHMENT 1

SAMPLE RULES OF BEHAVIOR

(DISCLAIMER – Any policy, procedure, or job description published or sponsored by the VAOCIS takes precedence over the contents of Appendix B. The guidance herein is for our use until superceded by VA.)

The following is a sample of a VBA field facility Rules of Behavior document. The document would be retained by the user, with the final page (signatures) removed and returned to the ISO.

These Rules of Behavior apply to all users of Veterans Affairs (VA) information technology (IT) systems.

1.1 Basic Orientation

1.11 Why Security Is Important For Everyone

All users of VA IT resources should be aware that any system potentially contains valuable and sometimes sensitive government and/or personal information, which must be protected to prevent disclosure, unauthorized changes, and loss. Each part of a system can introduce vulnerabilities to the whole, so protection must be consistent in order to be effective. On a larger scale, since VA IT resources are typically connected to VA and other sensitive government networks (e.g., Social Security Administration, Internal Revenue Service, Department of Defense), any system compromise is a potential threat on a grand scale to the Federal Government.

1.12 User Information and Contacts

This Information will be provided in a separate enclosure.

1.20 The VA IT Environment

1.21 General Information

a. All VA IT users must read and abide by these Rules of Behavior.

b. Users will process only data that pertains to official business. However, workstations may be used for limited personal use (i.e. reading on-line newspapers, checking bank accounts) as long as this use does not incur any cost to the government, does not violate any laws, regulation or standards, local VA or VBA policies, and the activity takes place during personal time (i.e., lunch time or after hours).

1.22 Sensitive Data Considerations

a. Unclassified but sensitive information on VA IT resources should be protected as For Official Use Only (FOUO). The following categories are examples of information that is normally FOUO:

c. Personal information subject to the Privacy Act of 1974, including Social Security number and benefits information.

d. Reports that disclose security vulnerabilities.

e. Information that could result in physical risk to individuals.

f. All output that contains FOUO information should be so marked or labeled by the user who generated the material, and then stored or transmitted with appropriate protection. The designation "For Official Use Only" should be marked, stamped or permanently affixed to the top and bottom of the outside of the front and back covers (if any), on the title page and on all pages of documents or information requiring such control. All diskettes or other magnetic media containing sensitive information should be similarly labeled and stored in locked containers (e.g., desks, filing cabinets, etc.).

g. Sensitive documents that are no longer needed should be shredded.

h. Magnetic media (e.g., diskettes and hard drives) that have been used for sensitive information may contain information even after the files are deleted. The information may be recoverable, even if a normal directory listing of the medium says it is empty. Before discarding magnetic media, users should do one of the following:

1. Degauss (erase all magnetic patterns on) the media.
2. Destroy the magnetic medium physically (open the plastic floppy disk casing, remove the disk, and shred it).
3. Use an approved software program to completely delete all files on the medium and overwrite them with ones and zeroes.

i. If you need assistance in disposing of magnetic media, consult your System Administrator or Information Systems Security Officer.

1.30 Passwords

a. Do not record your password in writing.

b. Do not share your password or accept another user's password if offered. Sharing passwords defeats the system's user identification and authentication mechanisms. In addition to sharing access privileges, participants share liability for any unauthorized behavior traced to the shared User ID and password.

c. Passwords will be a minimum of eight but not more than 15 characters in length.

d. Your password should be something you can easily remember.

e. Your password should not be something that another can guess so, do not use the name of your spouse, pets, or children, or words found in a dictionary.

f. Single-word passwords are susceptible to being guessed by software routines that check every word in the dictionary.

g. Use two small groups of alphabetical or numeric characters, or words, linked by a number or typographical character (&, *, !, etc.).

h. SAs have no way to look up your password. If you forget it, your SA will change it and make you pick a new password.

i. The system will prompt you will change your password every 90 days.

j. A new password cannot be one you used recently. Certain operating systems (i.e., Windows NT) remember as far back as the ten most recently used passwords.

k. If there is a reason, you may change your password before the end of 90 days, but only after three days have elapsed since the password to be changed was created. If there is a compelling reason to change the existing password before the end of the three-day period (such as a suspected compromise) contact the SA.

l. Users will be locked out of the system after six consecutive incorrect password entries and will be required to contact the SA.

m. Passwords are case sensitive. Users should not attempt to enter a password with the "caps lock" key enabled.

1.40 Electronic Mail

a. Government-provided electronic mail is intended for official and authorized purposes only. Electronic mail users must exercise common sense, good judgment, and propriety in the use of Government resources. While short personal messages are acceptable, parallel to the way Government telephones are sometimes used, other non-official uses are prohibited. Personal messages sent to groups of people are likely to fall into the category of prohibited use. Therefore, personal messages should not be sent to large groups. The presumption is that no notice except those sent by VA systems administrators or support personnel is so important that it should be broadcast globally to everyone within an organization or VA-wide without the approval of the appropriate office head. Broadcast messages are those sent to public groups listed (i.e., VBA, VHA, NCA, etc.) in the email software's address book or large personal groups.

b. Well intentioned notices including: retirements, deaths, births, lost or found property, or car lights left on, are not appropriate material for broadcast messages.

c. Employees are prohibited from using VA office automation or electronic mail systems to distribute information on any non-Government activities, including but not limited to: charitable events, religious observances, fund-raiser, and personal business. Employees who misuse Government resources in this way may have electronic mail privileges withdrawn and may be subject to disciplinary action.

Government employees should have no expectation of privacy when using the VA mail system. Electronic mail is not confidential. SAs may read the electronic mail of others (for a specific purpose) with appropriate authorization. In addition, technical or administrative problems may create a situation in which it is necessary for an

administrator or system manager to read message text. Moreover, VA views electronic mail messages to be Government property, and officials may have access to those messages whenever there is a legitimate Government purpose for such access. Users should treat the electronic mail system like the use of Government-provided inter-office mail system.

d. Do not use government email to send personal or official email to your home, friends, or other recipients outside the VBA network that contains sensitive data, e.g. SSNs, personal addresses, etc. Data sent outside VA over the public network is protected.

1.50 Internet Use

It is VA policy to safeguard VA data and reduce unnecessary risks to the integrity, availability, and confidentiality of VA computer and communication resources that may arise because of Internet abuse and misuse. This policy governs the activities of VA Internet users, but does not address Internet security.

1.51 General Policy

a. VA information systems will be used for only official Internet use and authorized personal Internet use. Official Internet use means that VA information systems may be used to access Internet resources for official communication, research, or professional development, as long as this access relates to the VA mission. Authorized personal Internet use means that with the permission of the VA, Internet resources may be accessed for authorized personal use either before or after work hours, during lunch periods, or during other authorized breaks during the day.

b. Authorized personal use applies to all government personnel and, at the discretion of the VA, may be extended to contractor personnel working in VA facilities.

c. In no case will the personal use of government resources be allowed to interfere with the VA mission, pose a hazard to the security of government data or resources, or reflect adversely on the VA or the Federal Government. The VA may revoke the privilege of authorized personal use at any time for any perceived misuse of government resources.

1.52 Prohibited Internet Uses

The following are prohibited uses of the Internet:

a. Possessing or distributing child pornography is a federal crime. Anyone caught with child pornography on a government computer will be prosecuted. VA does not recognize any legitimate reason for the use of pornography of any sort. Accessing any pornographic site is considered fraud, waste, and abuse of government resources and will be reported to the local network support and ISO.

b. Accessing, transmitting, storing, or distributing offensive material (e.g., racist literature, material, or symbols).

c. Participating in "chat room" discussions that are not for official business.

d. Accessing known "hacker" sites and downloading hacking tools without special authorization.

e. Lobbying or advocacy on behalf of any political organization or religious group not affiliated with the VA.

f. Viewing, damaging, deleting, or interfering with the functioning of any system or any other person's files or communications.

g. Conducting Internet activities for personal or commercial financial gain, along with unauthorized fund-raising. Fund-raising for certain government-approved organizations may be authorized by VA.

h. Attempting to circumvent or disable any Internet security or auditing system without prior authorization from the ISO or SA. This includes disabling virus detection mechanisms and modifying or altering the operating system of the hardware used to connect to the Internet.

i. Downloading, installing, storing, or using the software from the Internet in violation of any patent, copyright, or license agreements is prohibited. All files downloaded from the Internet must be scanned using approved antivirus software before they are opened, executed, or forwarded to other users.

1.53 Transmission of Data Over the Internet

Transmission of data over the Internet requires the use of appropriate safeguards. Sensitive and "FOUO" information must not be transmitted over the Internet unless appropriate safeguards (e.g., encryption) have been implemented. Since these safeguards are not available to VBA end-users, transmission of sensitive and "FOUO" information outside the VA's Wide-Area Network (i.e. via Internet) is prohibited.

1.54 Multiple User Computer Systems Used for Internet Access

Not applicable

1.55 Dial-Up Access to the Internet Using a Modem

Dial-up access to the Internet is prohibited for users connected to the VA information systems.

1.60 Web Page Establishment and Maintenance

Not applicable

1.70 Interacting With Administrators

a. Occasionally, users need to call upon administrators at various levels in order to obtain services or meet requirements for a specific task. Some routine occasions are listed below.

b. When you start a new job, or your job description changes, coordinate your VA IS access requirements and parameters with your first line supervisor.

c. When you need to obtain membership in a shared directory, or change or terminate your membership privileges, see the owner of that directory.

d. When you need other access privileges in order to do your job, notify your supervisor.

e. When you find that your access to VA resources is beyond what you need to do your job, notify your supervisor.

f. When you need to remove any computer resource from VA premises, see your supervisor for approval and a hand receipt. Resources may only be removed from VA premises for official use.

1.80 Configuration Management

1.81 Things You May Change

You may change the Windows "wallpaper" background (using one of the standard, system-provided backgrounds).

1.82 Things You May Not Change

a. Do not install any software onto your workstation or any other VA system resources. Only the VA SA (or his/her designated representative) is authorized to load software on workstations or servers.

b. Do not attempt to add printers to the ones your workstation can select. If you need access to another printer, see your supervisor or SA. Normally, users will be assigned to the printer nearest to their workstation area.

c. Do not add any additional hardware or peripheral devices to any workstation, server or other system resource. This includes all devices such as extra memory, hard drives, printers, scanners, additional servers, additional processors, etc. These tasks are handled by the SA and subject to configuration control.

1.90 Unauthorized Activities

All VA IT system users are held strictly accountable for their actions while on the system. User activity may be monitored and system activity audited to detect unauthorized behavior. Unauthorized activity may result in a warning, reprimand, loss of access, formal disciplinary action (including dismissal), or even legal action (such as a fine or imprisonment).

Unauthorized activities include:

a. Entering unauthorized, inaccurate, or false information. Do not delete or manipulate information inappropriately.

b. Using data for which you have not been granted authorization. Do not explore data or IS capabilities that are not related to your job or attempt to access information which you do not have authority to access. If you have any questions about the limits of your authorization, consult your supervisor for clarification.

c. Retrieving information for someone who does not have access to it himself/herself, except as specifically authorized:

    1. In your job description.

    2. By your supervisor.

d. Violating copyright and site licenses of proprietary software. This may happen when multiple copies of licensed software is installed, as well as when unlicensed software is installed.

e. Installing unauthorized software. Do not install outside software (including other agency software, shareware, freeware, personally purchased, or pirated software) on a VA system.

f. Installing modems (either internal or external) on a workstation, server or any other VA system resource. Although covered in the preceding section on configuration management, modems deserve special attention because they are a well-known way to bypass firewall protection. In particular, modems that are set to answer calls enable system access from outside the facility and may be regarded as a malicious breach of security.

g. Storing or processing classified national security information on a VA system. If, for any reason, classified information is introduced to a VA system, notify your SA as soon as possible.

h. Leaving your computer logged in to the VA network, but unprotected. Log-off your workstation whenever you are away from the immediate work area, unless a screen saver feature with a password enabled is properly invoked.

2.00 Your Role In Protecting the VA IT System Resources

a. Ensure that any data that is visible on the workstation monitor screen cannot be viewed by unauthorized personnel.

b. Invoke an appropriate level of protection whenever you leave your workstation unattended. For short periods, (visiting the restroom, or retrieving output from a printer that is out of sight of your workstation) you may use a password-protected screen saver feature. For longer periods, (going to another floor or leaving the building), log-off the workstation. The following guidelines will be followed when using the screen saver option:

    1. Only screen savers provided with the system (e.g., Microsoft Windows) are authorized. No other screen savers are to be installed.

    2. The password option for the screen saver must be invoked by the user. The password created will be generated by the user. The criteria for generating

that password will be the same as that used for creating a VA network log-on password. The screen saver password must not be the same password used for logging on to other VA networks and systems.

3. The user will ensure that the screen saver activates before leaving the workstation unattended. This must be done, because there are conditions in a session that will delay or preclude the screen saver from activating (the print pop-up is present on the screen, data exchanges are occurring between server and workstations, etc.).

c. Ensure printouts are retrieved as soon as possible. Output should not be left unattended for any longer than is necessary.

d. Protect your equipment (workstation, diskettes, etc.) from physical damage. Ensure that your workstation is clean, ventilated, and located in a place where it is not likely to be bumped or knocked over. Keep food and drinks where they won't get spilled on the equipment.

e. Safeguard VA resources against waste, loss, abuse, unauthorized use, and misappropriation.

f. Scan all disks for viruses before use, especially if they are received from external sources. Discontinue use of any VA IS resources that show indications of being infected by a virus and immediately report any incidents to the ISO.

g. Report any security incidents or suspected security incidents, including computer virus infections, to your ISO. The term "security incident" includes any event that may result in the disclosure of sensitive information to unauthorized individuals, or that results in unauthorized access, modification or destruction of system data, loss of system processing capability, or loss or theft of any computer system media.

h. Challenge any unauthorized personnel in your work area.

2.10 Signature

SYSTEM ACCESS AGREEMENT

(Return to Information Security Officer)

1. I have read, understand, and will comply with the Rules of Behavior for users of VA information systems dated January 6, 2005. I have retained a copy of the Rules of Behavior for personal reference.
2. I understand that the policies and requirements set forth in this System Access Agreement and the Rules of Behavior are subject to change without prior notice. I further understand that I am responsible for keeping abreast of and complying with changes to these policies and procedures as they are announced. I am also responsible for compliance with any supplemental local security policies, which are established and announced by station management.
3. By using these systems following authorization and establishment of an account pursuant to an appropriately submitted access request, I reconfirm my agreement to comply with the Rules of Behavior, System Access Agreement, and other policies and procedures governing use of those systems. This agreement includes my consent to review and actions including (but not limited to) monitoring, recording, copying, auditing, inspecting, investigating, restriction of access, blocking, tracking, disclosure to authorized personnel, or any other necessary management and control actions performed by authorized VA and law enforcement personnel.
4. Information contained in these systems is subject to the provisions of various Federal statues, including the Privacy Act (5 USC 552a) and veterans records confidentiality statues such as 38 USC 5701 and 7332. Access to this information is on a need-to-know basis.
5. I am prohibited from attempting or allowing others (knowingly or through my negligence) to attempt to (a) access, upload, change or delete information contained in these systems, (b) modify these systems, (c) deny access to these systems, (d) deny access to resources of these systems through unauthorized use, or (e) otherwise misuse these systems.
6. If I (a) have been granted access to VBA systems via Virtual Private Network or other remote connection, (b) work at home or at another off-site location and bring files to the office for upload to VBA systems, or (c) access VBA systems in a way that does not invoke automatic update and application of VBA virus and security measures, I acknowledge that it is my responsibility to ensure that my remote equipment meets VBA equipment software, hardware and security standards, to include being updated with current virus protection. I understand that I may be required to provide periodic verification of this compliance, and that failure to meet the requirements or to submit a report could lead to temporary or permanent revocation of my system access authorization.

Signature	Date
Employee Name (Print)	Organizational Symbol and Telephone

House Committee on Veterans Affairs
Disability Assistance and Memorial Affairs Subcommittee
and
Economic Opportunity Subcommittee

Joint Oversight Hearing on Information Technology Security

June 20, 2006

Questions from Congresswoman Berkley

Question 1: According to the IG reports and testimony, a number of VBA's security vulnerabilities will be corrected by the deployment of VETSNET. Please describe in detail the current status of VETSNET and the next five milestones to be achieved including relevant dates.

Response: VETSNET will replace the legacy Compensation and Pension system and includes the following major applications:

1. Modern Award Processing- Development (MAP-D) – to support claims establishment, development of claims, and workflow tracking.
2. Rating Board Automation (RBA) 2000 – to support the rating and evaluation of disability claims.
3. SHARE/Search and Participant Profile – to record and update basic information about veterans and their dependents in the corporate and legacy databases.
4. Financial Accounting System (FAS) – to support generation and audit of benefit payments.
5. Award -- to prepare and calculate benefit awards.

The first three applications are being used today by all veterans service representatives (VSRs) and rating veterans service representatives (RVSRs) in each regional office (RO) as the basis for claims processing. All five VETSNET applications are being used by the Lincoln and Nashville ROs to pay electronic funds transfer disability compensation claims for veterans who are rated from 0 percent through 100 percent disabled (except for apportionments, and other low-volume types of payment offsets). All other ROs are currently processing compensation claims which are being denied, or where service connection has been granted at the 0 percent through 20 percent level.

In 2005, Carnegie Mellon's Software Engineering Institute (SEI) was commissioned to provide an Independent Technical Assessment (ITA) of the VETSNET project. In SEI's final report, published in January 2006, SEI concluded that the VETSNET project should continue, but changes to the overall management of the project are needed. MITRE Corporation, a Federally funded research and development corporation, has been engaged to assist VBA in identifying and executing these changes.

One significant area highlighted by SEI is the need for an integrated schedule and comprehensive release plan to document all actions necessary to complete the VETSNET C&P project. As part of its contract, MITRE Corporation was actively

involved with VBA leadership in formulating such a plan. This *Integrated Schedule and Release Plan* was completed in August 2006. Briefings on the plan for VA officials are currently being scheduled and conducted. When the plan is approved by the Secretary, the House and Senate Committees on Veterans' Affairs will be provided information on its contents and the timeline for completing remaining tasks.

Question 2: When will VETSNET be fully deployed?

Response: The *Integrated Schedule and Release Plan* details the actions necessary to complete the VETSNET C&P project. Briefings on the plan for VA officials are currently being scheduled and conducted. When the plan is approved by the Secretary, the House and Senate Committees on Veterans' Affairs will be provided information on its contents and the timeline for completing remaining tasks. This plan does not specifically address other benefit programs such as Vocational Rehabilitation and Employment (VR&E) and Education. However, we are working with these benefit programs to specifically address their business requirements. This will ensure their successful migration from the Benefit Delivery Network while addressing their business needs.

Question 3: Are there any interim measures which should be taken to enhance data security while VETSNET continues to be developed?

Response: As a result of recommendations from the Office of Inspector General (OIG), changes have already been made to the Benefits Delivery Network systems. For example, strong security passwords with 30 day expirations have been implemented. Procedures regarding employee position changes have been strengthened to ensure that an employee's system access rights are reviewed and modified according to their assignments and properly removed upon termination or change in assignment.

VBA Network Support Centers (NSCs) perform annual audits of security password files at each regional office.

VBA is also in the process of replacing file transfer protocols with secure protocols. In addition, file transfer protocols have been restricted to a limited number of administrative accounts. Only one-way transactions are allowed, which helps prevent a user from sending malicious files to the server.

Other efforts that are underway or scheduled include the following.

- The Office of Information and Technology has intensified efforts to determine enterprise encryption requirements for all sensitive data throughout the Department and plans to have an implementation strategy by the end of the calendar year. In the interim, the Office of IT Field Security Operations is working with the administrations to increase the applications of Public Key Infrastructure (PKI) certificates to protect sensitive e-mail transmissions.

- Encryption standards have been developed for VA-controlled laptops as directed by Office of Management and Budget (OMB). All laptops will undergo a security

review to ensure that all security and virus software is current and that encryption software is installed, to be completed by September 15, 2006.

- The Department of Veterans Affairs (VA) will upgrade all VA computers to the XP Operating System and upgrade peripheral devices as necessary. This effort is included in VA's fiscal year (FY) 2007 budget and completion is targeted for the end of FY 2007.

An extensive effort is underway to improve the VA's performance regarding background investigations - with special emphasis on those positions requiring extensive access to sensitive information and computer systems/networks. VA is working aggressively to resolve problems that have existed for some time with background investigations. One of the improvements is the use of the Electronics Questionnaires for Investigations Processing (e-QIP), an OPM sponsored system designed to allow electronic completion and submission of all personnel investigation forms to OPM for completion of the investigations. VA is actively involved in the implementation of e-QIP. The current schedule will result in over 70 percent of VA facilities using e-QIP by December 31, 2006, and 100 percent by March 2007.

Question 4: How are audit functions performed in VETSNET development? Is there a dedicated, independent staff responsible for audit functions?

Response: On July 11, 2002, VBA initiated a contract supporting functional and technical end-to-end processing capabilities to ensure accurate and timely benefit payments are made. This testing validates each VETSNET function and verifies end-to-end system capability. Independent functional and technical end-to-end testing is currently conducted by Science Applications International Corporation (SAIC) on each VETSNET release prior to deployment to production.

Question 5: Does VBA have sufficient qualified personnel to address the deficiencies identified by the IG?

Response: VBA will work in coordination with the VA CIO on the remediation of the deficiencies identified by the OIG. VBA has sufficient qualified personnel to support the VA CIO in whatever capacity is required.

Question 6: Please provide the number and general job description of VA employees and contractors assigned solely to independent audit functions for VETSNET and the Benefits Delivery Network, and of any other software development staff working on veterans benefits matters.

Response: Twenty-five contract test engineers from SAIC are assigned to independent audit functions for the VETSNET applications. Eight government information technology specialists are assigned responsibility for independent audit functions for the Benefits Delivery Network (BDN).

Software development staffs at the Austin Systems Development Center, the Hines Information Technology Center and St. Petersburg Systems Development Center have

responsibility for maintenance and development of the VETSNET applications. These staffs consist of 39 government information technology specialists and 60 contractors from Northrup Grumman Information Technology, Inc.

BDN software and other Compensation, Pension and Education software are maintained by 56 government information technology specialists at the Hines Information Technology Center. Twenty-five test engineers from SAIC are assigned to independent audit functions for the VETSNET applications. Eight government information technology specialists are assigned responsibility for independent audit functions for the BDN.

Question 7: Has VBA replaced all computers and similar devices which are no longer supported by the manufacturer? If not, why not? If not, when will this be completed?

Response: While VBA has hardware that is no longer manufactured or has reached its "end of life" cycle, we have maintenance agreements to support the equipment that is in use. In addition, all VBA hardware (desktop computers, network servers, and routers) runs software that is currently supported by the software manufacturer. For these reasons, there is no immediate maintenance concern and no security vulnerability that would require us to replace the hardware.

Questions from Congressman Udall

Question 1: According to your testimony, each regional office has an information security officer. Is information security the only responsibility of these officers? Do the information security officers have regular communication among each other or group training sessions?

Response: Most information security officers (ISO) occupy full-time security positions. In the past, stations with fewer than 200 employees were authorized to have a part-time ISO who also had collateral duties. However, with the May 1, 2006 VA Information Technology (IT) realignment, all RO directors have been instructed that ISOs at all stations will be required to be available full time for security tasks effective October 1, 2006.

The ISOs regularly exchange ideas and information by attending monthly and quarterly discussion calls with Veterans Health Administration (VHA), National Cemetery Administration (NCA), and VBA. All ISOs who work at ROs received professional level training by attending special sessions at the annual four-day Information Security conference hosted by the VA Office of Cyber and Information Security (OCIS). Prior to May 1 of this year, VBA provided security guidance to the ISO through letters and hotline calls. Now that the ISOs are detailed to the OCIS and will be permanently reassigned in October, the ISOs obtain guidance through their district and regional ISOs.

Question 2: Please provide the specific actions which VBA has taken and the purchases made to remediate deficiencies identified by the IG and the cost of each remediation.

Response: VBA has worked closely with VA to strengthen and better manage security of VBA systems. The following installs were accomplished through the Department with no direct cost to VBA.

- VBA has installed Host Intrusion Protection Software (HIPS), designed to block undesirable/malicious network activity at the host level.

- VBA installed Harris STAT Guardian VMS Scanner in November 2005 on the RO desktops and servers for remote scanning and security patch management.

- VBA stations implemented Real Secure Desktop Protector (RSDP) agent in June 2006.

- VBA has installed RO Pest Patrol for prevention of malware issues and Password Policy Enforcer for strong passwords on system password files.

- Switch Port Security is currently being piloted at the Network Support Centers. This will enhance security by controlling access and eliminating security vulnerability risks when unauthorized devices are connected to network drops on the VBA local area network (LAN). Local administrators will also be able to enable/disable port security on selected ports and to enable/disable/block selected ports.

VBA has spent approximately $1.0M acquiring hardware to create a fully operational disaster recovery capability for the Philadelphia Information Technology Center Web Server. VBA currently anticipates making this site fully operational in December 2006.

VBA has completed verification of position sensitivity for all VBA employees and is proceeding with background checks in phases. VBA estimates approximately $1.0M will be needed to process background checks or for current employees who have none. An additional $2.0M will be needed to upgrade employees to higher certifications because their jobs changed.

VBA is finalizing a Computer Room Design Guide for new construction as a result of the physical security and fire protection issues with the computer rooms at the regional offices during Certification and Accreditation of VBA systems in FY 2005. The guide will establish security configuration standards for the regional office computer rooms, especially new construction. Deficiencies to remediate will be addressed through the minor construction budget.

VBA began implementing Public Key Infrastructure technology throughout VBA in June 2006 to protect the integrity and confidentiality of sensitive information exchanged by email within VA and between external recipients who do business with VA. In addition, VBA is participating in the VA Office of Cyber and Information Security (OCIS) evaluation of whole disk encryption to centrally manage encryption software for computers and removable devices to protect data files and backups. VBA is working

with VA network management to evaluate methods of encrypting transmissions across the network. This implementation entails no direct costs for VBA.

Questions from Congresswoman Herseth

Question 1: How much has VA expended on notices to veterans, call center operations and staffing, and any other activities related to the data breach? From what accounts are the funds being provided?

Response: VA expended $6,612,777 on notices to veterans. The Department adjusted priorities within the General Operating Expenses account to make the resources available for this project. Through July 12, 2006, VA had spent approximately $11.2 million on the call centers. Resources for the call centers were made available by reprogramming funds within the Information Technology Systems account.

Question 2: Will VA need additional funding in FY 2006 or FY 2007 to replace monies reprogrammed to cover the costs of addressing the ramifications of the data breach?

Response: VA will not need any additional funds to cover the costs incurred to date on sending notices to veterans or on the call centers. There will be no adverse impact on the delivery of services to veterans as a result of the funds the Department has already expended on these activities.

Question 3: According to the VA IG, computers of a certain age must continue to operate due to special document scanners associated with the Imaging Management System (TIMS). These scanners and computers are expected to be retired in FY 2006 if funds are available. Have these funds been made available?

Response: All VBA workstations are running the same operating system. The TIMS workstations are all running Windows 2000 and the desktops are all VBA standard workstations. The scanner problem was resolved by upgrading to Windows 2000. VBA is finalizing plans to migrate all PCs to Windows XP by January 2007.

Question 4: Is the Loan Guaranty Service contracting with any offshore contractors and, if so, are specific clauses included in the contracts to require recognition to the Privacy Act and any other applicable laws?

Response: Loan Guaranty Service is not directly contracting with any offshore contractors. However, both the portfolio loan servicing contract provider, Countrywide Home Loans (CHL), and the property management service contract provider, Ocwen Loan Servicing, LLC, use offshore labor for administrative functions.

Currently, CHL uses offshore labor located in India for functions such as information systems development and some back office functions. The Indian staff are employees of CHL rather than contract laborers, and use CHL proprietary systems. The contract between VA and CHL incorporates requirements of the Privacy Act, as well as stipulations that CHL's IT systems meet the minimum security requirements defined by

appropriate National Institute of Standards in Technology (NIST) standards; the Federal Information Security Management Act (FISMA); and other appropriate legislation. VA has read-only access to CHL's servicing system with the exception of the ability of certain employees to enter servicing notes. CHL has no direct access to any VA systems.

Ocwen uses offshore labor to perform administrative functions such as electronically processing invoices from sub-contractors, assisting a vendor with the application process to become an Ocwen sub-contractor, and electronically assigning appraisers to evaluate properties. Section 5.0 of the contract covers security requirements and disclosure of information. However, VA only provides property data to Ocwen. VA does not provide veteran data to Ocwen and Ocwen has no direct access to VA systems. Therefore, the Privacy Act is not referenced in the contract

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington DC 20420

JUL 12 2006

The Honorable Jeff Miller
Chairman
Subcommittee on Disability
Assistance and Memorial Affairs
Committee on Veterans' Affairs
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

This is in response to your and Chairman Boozman's letter of June 29, 2006, following the June 20, 2006, joint hearing before the Subcommittee on Disability Assistance and Memorial Affairs and the Subcommittee on Economic Opportunity. In your letter, you requested answers to several hearing questions.

Enclosed are the Office of Inspector General's answers to your questions. We thank you for the opportunity to provide this information for the hearing record. If you need additional information, please do not hesitate to contact the office. A similar response is being sent to Chairman Boozman.

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

Sincerely,

MICHAEL L. STALEY
Assistant Inspector General
for Auditing

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington DC 20420

JUL 12 2006

The Honorable John Boozman
Chairman
Subcommittee on Economic Opportunity
Committee on Veterans' Affairs
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

This is in response to your and Chairman Miller's letter of June 29, 2006, following the June 20, 2006, joint hearing before the Subcommittee on Disability Assistance and Memorial Affairs and the Subcommittee on Economic Opportunity. In your letter, you requested answers to several hearing questions.

Enclosed are the Office of Inspector General's answers to your questions. We thank you for the opportunity to provide this information for the hearing record. If you need additional information, please do not hesitate to contact the office. A similar response is being sent to Chairman Miller.

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

Sincerely,

MICHAEL L. STALEY
Assistant Inspector General
for Auditing

Enclosure

1. With the current set-up at the Veterans Benefits Administration, where does the control for information technology lie? How does this affect security?

Prior to VA's decision to move towards a "federated IT system" the Veterans Benefits Administration (VBA) retained its own Chief Information Officer (CIO) and staff to oversee and provide technical assistance for all regional offices, the Hines, IL, Information Technology Center, and Philadelphia, PA, Information Technology Center. All decisions affecting security were the responsibility of the VBA CIO. The former VA CIO informed us that it was difficult to implement nationwide policies and procedures because of the decentralization of each administrations' information technology functions and that Information Security Officers (ISOs) did not report directly to the VA CIO, but rather to managers in each of the administrations. This decentralized approach has resulted in inconsistent interpretations in applying information security policies and procedures.

VA's decision to move towards a "federated IT system" has recently prompted action to temporarily reassign many of the VBA information technology employees to the VA's CIO. VA is currently developing policies and procedures for realigning operations and maintenance functions under the authority of the VA CIO, but plans to retain certain decentralized program development functions in the administrations. We will need to study the impact of these new policies and procedures to determine the extent ISOs will now directly report to the VA CIO, and how security will be affected by them.

2. In the past, your office has found instances where terminated or separated employees retained access to critical systems identified at various locations. Whose responsibility is it to ensure that former employees don't have access to computer systems or paper files?

We could not find any specific national policy that assigned notification and action responsibilities to managers at VA facilities. However, our reviews of local practices found that there is a shared responsibility among the managers releasing the employees, managers transferring the employees from one unit to another, human resources management, and the ISO at each facility. Communication among these responsible officials is essential for ensuring that the changing status of employees are reported timely to the ISO so that actions can be taken to cancel or modify computer access rights to information and data.

3. VA has opposed HR 4061 passed by the House and chosen to adopt what they call a federated model as opposed to the fully centralized model that would be mandated by HR 4061. Do you believe that the federated model will be more effective than centralized model in improving the overall management of VA information technology programs?

OIG and Government Accountability Office reports published over the years have shown the need for a centralized approach to reduce information security inconsistency and achieve standardization in and among all of the administrations. VA informed Congress that it plans to move towards a "federated IT system" to realign department-wide IT operations and maintenance responsibilities under the direct authority of the CIO. The main feature of the

realignment will place VA's IT budget, along with IT professionals involved in operations and maintenance work, directly under the authority of the VA CIO. However, IT employees involved in system development will remain under their respective administrations and staff offices.

Given that the planned realignment has just begun, VA's "federated IT system" implementation plans will need further study. For example, we will need to review whether existing IT systems and operations under the purview of the CIO will efficiently and effectively communicate with newly designed applications implemented by these system development offices. Failure to implement sound policies and procedures could introduce a significant amount of risk into the production environment if the access controls given to development staffs are not adequately developed and enforced.

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington DC 20420

JUL 12 2006

The Honorable Shelley Berkley
Ranking Democratic Member
Subcommittee on Disability Assistance
and Memorial Affairs
Committee on Veterans' Affairs
U.S. House of Representatives
Washington, DC 20515

Dear Congresswoman Berkley:

This is in response to your and Congresswoman Herseth's letter of June 29, 2006, following the June 20, 2006, joint hearing before the Subcommittee on Disability Assistance and Memorial Affairs and the Subcommittee on Economic Opportunity. In your letter, you requested answers to four hearing questions.

Enclosed are the Office of Inspector General's answers to your questions. We thank you for the opportunity to provide this information for the hearing record. If you need additional information, please do not hesitate to contact the office. A similar response is being sent to Congresswoman Herseth.

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

Sincerely,

MICHAEL L. STALEY
Assistant Inspector General
for Auditing

Enclosure

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington DC 20420

JUL 12 2006

The Honorable Stephanie Herseth
Ranking Democratic Member
Subcommittee on Economic Opportunity
Committee on Veterans' Affairs
U.S. House of Representatives
Washington, DC 20515

Dear Congresswoman Herseth:

This is in response to your and Congresswoman Berkley's letter of June 29, 2006, following the June 20, 2006, joint hearing before the Subcommittee on Disability Assistance and Memorial Affairs and the Subcommittee on Economic Opportunity. In your letter, you requested answers to four hearing questions.

Enclosed are the Office of Inspector General's answers to your questions. We thank you for the opportunity to provide this information for the hearing record. If you need additional information, please do not hesitate to contact the office. A similar response is being sent to Congresswoman Berkley.

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

Sincerely,

MICHAEL L. STALEY
Assistant Inspector General
for Auditing

Enclosure

Questions from Ranking Member Berkley for Mr. Staley:

1. VBA has identified VETSNET as a solution to some of the data security problems the IG has identified. Should VBA be taking any action to improve security on an interim basis where VETSNET is considered the ultimate solution?

The VETSNET initiative is currently under review by an external contractor, the MITRE Corporation. Veterans Benefits Administration (VBA) officials informed us the contractor's technical and risk management report should be completed in September 2006, and we plan to review the results of the work conducted by the MITRE Corporation early in fiscal year 2007. At that time, we will be able to evaluate whether VETSNET will provide the ultimate solution to VBA's security issues

2. What procedures existed on May 3, 2006, to notify the IG when VA experiences a loss of data?

There was no specific VA policy in place at the time of the incident that required reporting the loss of data to the OIG. Our report, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans,* dated July 11, 2006, addresses this topic further.

3. What procedures should exist to notify the IG whenever VA experiences a loss of sensitive data?

We are currently working with VA in identifying such procedures. At a minimum, VA must issue a policy clearly delineating a process for reporting incidents through the chain of command and to the appropriate law enforcement authorities within specific timeframes. To ensure that issues referred to the OIG are promptly addressed, OIG staff prepared and issued a checklist to VA identifying the specific information that should be provided with any notification.

As the result of this incident and work conducted by the OIG, actions are being taken to reevaluate the adequacy of VA's management/incident reporting process. The OIG has been contacted by the VA Office of Cyber and Information Security, in their effort to review and strengthen these procedures where applicable. VA has issued a draft "Concept of Operations for Incident Response" for comment which we are currently reviewing.

Questions from Congressman Udall for Mr. Staley:

4. According to your testimony, you mentioned that correction of deficiencies would be accomplished "if funds are available." To what extent has the lack of funds contributed to the deficiencies you have noted in such areas as perimeter security, old hardware and legacy applications?

The FISMA database retained by the VA CIO contains the assessment surveys of VA's major applications and systems. System and application deficiencies, as well as funded and unfunded remediation costs, are reported and stored in this database. Consequently, this database needs to

accurately demonstrate the security posture of VA's systems and major applications and the costs to remediate vulnerabilities. Also, it should accurately depict the risk of loss of the critical and sensitive information contained within these systems and major applications. Test comparisons of the sites visited to the entries in the FISMA database retained by the CIO found that not all information was accurate. While it may be that individual administrations have better estimates of their needs, the information in the CIO FISMA database was incomplete making it unfeasible to determine the full scale of funding necessary to remediate VA's information security vulnerabilities.

During our reviews, managers have told us that the unavailability of funding has been a factor in taking steps to improve inadequate perimeter security. Examples given include an insufficient number of police officers on duty, lack of camera coverage, and inadequate perimeter fence protection. VBA continues to use Windows 95/98 applications that do not provide necessary security protections. Compliance with existing policy and procedures for strengthening access controls, segregating duties, developing and implementing comprehensive contingency plans, and training should not involve significant funding considerations. However, we have not been able to find a comprehensive set of estimates on the amount of funding that will be needed to address all of the issues identified in our reports such as patch management solutions, encryption solutions, background checks, and upgrading aging operating systems and legacy systems to remediate information security vulnerabilities.

United States Government Accountability Office
Washington, DC 20548

July 14, 2006

The Honorable Jeff Miller
Chairman, Subcommittee on Disability Assistance
And Memorial Affairs
Committee on Veterans' Affairs
House of Representatives

The Honorable John Boozman
Chairman, Subcommittee on Economic Opportunity
Committee on Veterans' Affairs
House of Representatives

Subject: *Veterans Affairs: Subcommittees' Post-Hearing Question Concerning the Organizational Structure of the Department's Office of Information Technology*

This letter responds to your June 29, 2006, request that we address a question relating to our testimony of June 20, 2006.[1] At that hearing, we discussed the Department of Veterans Affairs information security program—including weaknesses reported by us and by others—as well as actions that the department has taken to address past recommendations. We also discussed potential measures that federal agencies can take to help limit the likelihood of personal information being compromised, and we identified key benefits and challenges associated with effectively notifying the public about security breaches. Your question and our response follow:

> *VA has opposed HR 4061 passed by the House and chosen to adopt what they call a federated model as opposed as to the fully centralized model that would be mandated by HR 4061. Do you believe that the federated model will be more effective than centralized model in improving the overall management of VA information technology programs?*

Improvement in the overall management of VA information technology programs will largely depend on extensive top management commitment to IT governance and processes in order to achieve maximum benefits. Management support is necessary to enable the Chief Information Officer (CIO) to apply information technology to VA's business needs, effectively manage the information technology infrastructure, and improve the department's accountability for IT resources. It will only be through this strong management commitment that VA can expect to succeed, whether it uses either the centralized or federated model. As we noted in our testimony on

[1] GAO, *Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs*, GAO-06-897T (Washington, D.C.: June 20, 2006).

September 14, 2005,[2] the realignment of VA's organizational structure holds promise for building a more solid foundation for investing in and improving the department's accountability for IT resources.

To enhance the effectiveness of VA's IT organization, the Deputy Secretary requested that the CIO perform a study of the existing organization, using outside assistance if necessary. In December 2004, VA contracted with Gartner Consulting[3] to conduct an organizational assessment of its IT program and recommend a new organizational model that would provide for greater efficiencies, economies of scale, and added business value. After analyzing VA's existing information technology environment, Gartner concluded that two organizational models—the centralized and the federated—offered the greatest potential for improving VA's IT management.

According to Gartner, under the centralized model, all information technology activities would be organized into a single entity that reports to VA's CIO. Key functional entities reporting directly to the CIO would include business applications, infrastructure and operations, enterprise architecture, data and information management, security management, and IT finance. According to Gartner, under the federated model, activities such as centralized planning, technology operations of data centers and networks, IT budgeting and financial activities, and security management would also be controlled by the CIO. However, business applications would be developed and supported by application teams in each business line—each of the three VA administrations would be considered a business line. Under the federated model, a governance process with strong IT investment management practices would also help guide the alignment between the CIO and the administrations.

While Gartner determined that either organizational model would improve VA's IT management, Gartner recommended the centralized model to VA for several reasons.

- The centralized model would require a shorter time frame to attain benefits similar to those offered by the federated model.
- The centralized model would offer more efficient realization of value for veterans.
- The centralized model would be stronger than the federated model in executing OneVA mission objectives.[4]

---

[2]GAO, *Veterans Affairs: The Critical Role of the Chief Information Officer Position in Effective Information Technology Management*, GAO-05-1017T (Washington, D.C.: Sept. 14, 2005).

[3] Gartner Consulting provides independent research and analysis for the Information Technology (IT) industry.

[4]VA's 2001-2006 Strategic Plan has four strategic goals and one enabling goal. The strategic goals are: (1) Restore the capability of disabled veterans. (2) Ensure a smooth transition for veterans from active military service to civilian life. (3) Honor and serve veterans in life and memorialize them in death. (4) Contribute to the public health and socioeconomic well being. The enabling goal, which represents crosscutting activities that enable all VA units to carry out the department's mission, focuses on the delivery of One VA world-class service to veterans and their families through effective communication and management of people, technology, business processes, and financial resources.

Gartner identified benefits and risks associated with the implementation of each of the models. Table 1 provides a summary of Gartner's respective benefits and risks of the two models.

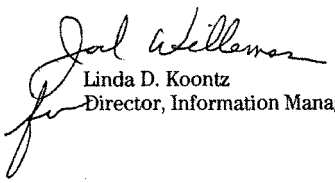
Table 1: Benefits and Risks Identified by Gartner for Federated vs. Centralized Models

	Federated Model	Centralized Model
Benefits	Allows business leaders to develop the application portfolio unique to their missions; achieve economies of scale across all VA by managing the infrastructure through a central function (assuming the consolidation of physical assets); and allowing the business unit IT team to be responsive to Administration mission demands.	Provides the greatest opportunity to successfully execute OneVA mission objectives; it maximizes asset utilization and achieves economies of scale across all VA by managing the infrastructure through a central function; and through common organization will more rapidly mature the IT investment management process across VA's IT program portfolio.
Risks	Includes difficulty in attaining OneVA mission objectives because of the defined barriers in culture, unaligned investment priorities across Administrations, and differences in technology and process which hinders effort to create veteran-centric systems. This approach also requires sustained executive commitment to IT investment management process (unattained to date within VA), is a significant scope of change to manage given the intended consolidation of physical assets and is deemed a modest organization disruption.	The potential risks from implementing this model are of course the significant organizational disruption and scope to manage. It also increases the complexity for the centralized organization to align its resources with Administration mission priorities and requires strong user orientation to be successful which is not in place at VA.

Source: Gartner Consulting

In light of the subcommittees' concerns regarding the recent security breach at VA, it should be noted that both the centralized and federated models would provide a structure that could improve VA's information security management. Under both models the function of the Security Management Office would be essentially the same. This office would be responsible for developing, maintaining, and publishing VA's enterprise information security standards, procedures, and guidelines. Under either model, responsibility for implementing security policies and procedures would rest in the operations domain under the CIO's authority. Therefore, for either model to successfully address VA's information security weaknesses will require strong leadership, sustained management commitment, disciplined processes, and consistent oversight.

We are sending copies of this letter to the Secretary of Veterans Affairs and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-6240 or by e-mail at koontzl@gao.gov. Key contributors to this correspondence include Barbara S. Oliver, Martin A. Katz, J. Michael Resser, and Eric L. Trout.



Linda D. Koontz
Director, Information Management Issues

(310776)

United States Government Accountability Office
Washington, DC 20548

July 21, 2006

The Honorable Shelley Berkley
Ranking Minority Member
Subcommittee on Disability Assistance
and Memorial Affairs
Committee on Veterans' Affairs
House of Representatives

The Honorable Stephanie Herseth
Ranking Minority Member
Subcommittee on Economic Opportunity
Committee on Veterans' Affairs
House of Representatives

Subject: *Veterans Affairs: Subcommittees Post-Hearing Questions Concerning Veterans Benefits Administration's Veterans Service Network (VETSNET)—a Replacement Compensation and Pension Benefits Payment System*

This letter responds to your June 29, 2006, request that we address questions relating to our testimony of June 20, 2006.[1] At that hearing, we discussed the information security program of the Department of Veterans Affairs, including weaknesses reported by us and by others, as well as actions that the department has taken to address past recommendations. We also discussed potential measures that federal agencies can take to help limit the likelihood of personal information being compromised, and we identified key benefits and challenges associated with effectively notifying the public about security breaches. Your questions, along with our responses, follow:

1. *Please provide a history of VETSNET activity.*

The VETSNET effort grew out of an initiative begun by the Veterans Benefits Administration (VBA) in 1986 to replace its outdated Benefits Delivery Network (BDN). The BDN, parts of which were developed in the 1960s, contains over 3 million veterans benefits records, including records related to compensation and pension, education, and vocational rehabilitation and employment. Originally, the plan was to modernize systems dealing with all these records and in so doing provide a rich source for answering questions about veterans' benefits and enable faster processing

[1] GAO, *Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs*, GAO-06-897T (Washington, D.C.: June 20, 2006).

of benefits. As envisioned in the 1980s, the modernization would produce a faster, more flexible, higher capacity system that would be both an information system and a payment system. In 1996, after experiencing numerous false starts and spending approximately $300 million on the overall modernization of BDN, VBA revised its strategy and narrowed its focus to modernizing the compensation and pension payment system.

At that time, we undertook an assessment of the department's software development capability[2] and determined that it was immature. In our assessment, we specifically examined the VETSNET effort and concluded that VBA could not reliably develop and maintain high-quality software on any major project within existing cost and schedule constraints. VBA showed significant weaknesses in requirements management, software project planning, and software subcontract management, with no identifiable strengths. We also testified that (1) VBA did not follow sound systems development practices on VETSNET, such as validation and verification of systems requirements; (2) it employed for the project a new systems development methodology and software development language not previously used; and (3) it did not develop the cost-benefit information necessary to track progress or assess return on investment (for example, total software to be developed and cost estimates).[3] As a result, we concluded that VBA's modernization efforts had inherent risks.

Between 1996 and 2002 we reported several more times on VETSNET, highlighting concerns in several areas. (See attachment 1 for description of the results of our products on this topic.) In these products, we made several recommendations aimed at improving VA's software development capabilities, including that the department take steps to achieve greater maturity in its software development processes[4] and that it delay any major investment in software development (beyond that needed to sustain critical day-to-day operations) until it had done so. In addition, we made recommendations aimed specifically at VETSNET development, including that VBA assess and validate users' requirements for the new system; complete testing of the system's functional business capability, as well as end-to-end testing to ensure that payments are made accurately; and establish an integrated project plan to guide its transition from the old to the new system.

Although VBA took various actions in response to these recommendations, we continued to identify the department's weak software development capability as a significant factor contributing to VBA's persistent problems in developing and implementing the system. We also reported that VBA continued to work on VETSNET without an integrated project plan. As a result, the development of VETSNET

---

[2] GAO, *Software Capability Evaluation: VA's Software Development Process Is Immature*, GAO/AIMD-96-90 (Washington, D.C.: June 19, 1996).

[3] GAO, *Veterans Benefits Modernization: Management and Technical Weaknesses Must Be Overcome If Modernization Is to Succeed*, GAO/T-AIMD-96-103 (Washington, D.C.: June 19, 1996).

[4] Specifically, we recommended that it achieve the repeatable level of process maturity; at this level, basic project management processes are established to track cost, schedule, and functionality, and the necessary process discipline is in place to repeat earlier successes on projects with similar applications.

continued to suffer from problems in several areas, including project management, requirements development, and testing.

Our most recent review of the VETSNET initiative was in 2002.[5] At that time, we offered a number of recommendations regarding the ongoing compensation and pension (C&P) replacement program.[6] We testified that VBA should assess and validate users' requirements for the new system and complete testing of the system's functional business capability, including end-to-end testing.[7] We also recommended that VA appoint a project manager, thoroughly analyze its current initiative, and develop a number of plans, including a revised C&P replacement strategy and an integrated project plan. We noted that VBA had much work to do before it could fully implement the VETSNET C&P system by its target date (at that time) of 2005, and thus it would have to ensure that the aging BDN would be available to continue accurately processing benefits payments until a new system could be deployed. Accordingly, we recommended that VBA develop action plans to move from the current to the replacement system and to ensure the availability of BDN to provide the more than 3.5 million payments made to veterans each month.[8]

VA concurred with our recommendations and took several actions to address them. For example, it appointed a full-time project manager. Also, the project team reported that to ensure that business needs were met, certification had been completed of users' requirements for the system's applications.

In addition, VA reported that a revised strategy for the replacement system was completed. This revised strategy included the business case, described the methodology used to identify system development alternatives, displayed the cost/benefit analysis results of the viable alternatives that could be used to develop the system, and provided a description of the recommended development plan. Based on this strategy, the Secretary of Veterans Affairs, Assistant Secretary for Information and Technology, the Under Secretary for Benefits, and the Deputy Chief Information Officer for Benefits approved continuation of the VETSNET development in September 2002. Further, to ensure that BDN would be able to continue accurately processing benefits payment until the new system was deployed, VBA purchased additional BDN hardware, hired 11 new staff members to support BDN operations, successfully tested a contingency plan in the event of disruption of the system, and provided retention bonuses to staff familiar with BDN operations.

---

[5] GAO, *VA Information Technology: Management Making Important Progress in Addressing Key Challenges,* GAO-02-1054T (Washington, D.C.: September 26, 2002).

[6] Since VBA has moved the focus of the VETSNET project to the C&P replacement in 1996, it has used both "VETSNET" and "compensation and pension replacement system" interchangeably in documents related to the replacement initiative.

[7] GAO, *VA Information Technology: Progress Made, but Continued Management Attention Is Key to Achieving Results*, GAO-02-369T (Washington, D.C.: Mar. 13, 2002).

[8] GAO, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, GAO-02-703 (Washington, D.C.: June 12, 2002).

However, VBA did not develop an integrated project plan for VETSNET, which is a basic requirement of sound project management. In addition, it did not develop an action plan for transitioning from the current to the replacement system. Thus, although the actions taken addressed some of our specific concerns, they were not sufficient to establish the program on a sound footing.

In 2005, the VA CIO became concerned about the continuing problems with VETSNET: the project continued to miss target dates, and costs continued to increase (VA indicated that by 2005 these costs exceeded $69 million). Accordingly, he arranged to contract for an independent assessment of the department's options for the VETSNET project, including an evaluation of whether the program should be terminated. This assessment, conducted by the Carnegie Mellon Software Engineering Institute (SEI), concluded that the program faced many risks arising from management, organizational, and program issues, but no technical barriers that could not be overcome.[9] According to SEI, terminating the program would not solve the underlying management and organizational problems, which would continue to hamper any new or revised effort.

SEI recommended that the department not terminate the program but take an aggressive approach to dealing with issues while continuing to work on the program at a reduced pace. According to SEI, this approach would allow VA to make necessary improvements to its system and software engineering and program management capabilities while making gradual progress on the system. SEI also discussed specific concerns about the system's management and the organization's capabilities, presenting areas that required focus regardless of the particular course that VA chose for the system. For example:

- VBA needed to set realistic deadlines. SEI commented that there was no credible evidence that VETSNET would be complete by the target date, which at the time of the SEI review was December 2006. Because this deadline was unrealistic, VBA needed to plan and budget for supporting BDN so that its ability to pay veterans benefits would not be disrupted.
- VBA needed to establish an effective requirements process. SEI reported that the current organizational layers between requirement sources and development resources result in delays and confusion.
- VBA needed to implement effective program measurements in order to assess progress.
- VBA needed to establish sound program management. According to SEI, different organizational components had independent schedules and priorities, which caused confusion and deprived the department of a program perspective.

These observations are consistent with our long-standing concerns regarding fundamental deficiencies in VBA's management of the project.

---

[9] Kathryn Ambrose, William Novak, Steve Palmquist, Ray Williams, and Carol Woody, *Report of the Independent Technical Assessment on the Department of Veterans Affairs VETSNET Program* (Carnegie Mellon Software Engineering Institute, September 2005).

In the wake of the SEI assessment and recommendations, VA is in the process of creating, with contract help, an integrated master plan that is to cover the C&P replacement project. Because the development of this plan is in process, no cost or schedule milestones have yet been finalized. According to VA, the integrated master plan is to be completed by the end of August 2006.

VA officials told us that they intend to complete this plan before beginning to plan for modernizing the systems for paying education benefits or for paying vocational rehabilitation and employment benefits. Plans for making the transition to VETSNET and ending VBA's dependence on BDN are also on hold.

Until it has an integrated project plan and schedule incorporating all the critical areas of the system development effort, VBA will lack the means of determining what needs to be done and when, and of measuring progress. Without plans to move from the current to the replacement system, VBA will lack assurance that it can continue to pay beneficiaries accurately and on time through the transition period.

2. *Can we reasonably expect that VETSNET will be deployed in a sufficient manner to address data security vulnerabilities in a timely fashion?*

As previously noted, VBA has not yet created an integrated master plan for the C&P replacement project. Until the integrated master plan—which should include an implementation plan with detailed work tasks, resources, and completion milestones—has been finalized, we will not have a basis for determining whether and how VETSNET deployment will address data security vulnerabilities.

We are sending copies of this letter to the Secretary of Veterans Affairs and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-6240 or by e-mail at koontzl@gao.gov. Key contributors to this correspondence include Barbara S. Oliver, Robert L. Williams, Jr., and Charles E. Youman.

Linda D. Koontz
Director, Information Management Issues

Attachment 1. Past GAO Products on VETSNET

We previously performed several reviews addressing VETSNET and made numerous recommendations aimed at strengthening the program and VA's software development and management capabilities. The table summarizes the results of these reviews.

GAO Products Highlighting Concerns with VETSNET Project to Replace Compensation and Pension (C&P) Payment System

Issuance date Report/testimony	Results of review
June 19, 1996 GAO/T-AIMD-96-103	VETSNET had inherent risks in that (1) it did not follow sound systems development practices, such as validation and verification of systems requirements; (2) it employed a new systems development methodology and software development language not previously used; and (3) VBA did not develop the cost-benefit information necessary to track progress or assess return on investment (for example, total software to be developed and cost estimates).
June 19, 1996 GAO/AIMD-96-90	VBA's software development capability was immature and it could not reliably develop and maintain high-quality software on any major project within existing cost and schedule constraints, placing its software development projects at significant risk. VBA showed significant weaknesses in requirements management, software project planning, and software subcontract management, with no identifiable strengths.
May 30, 1997 GAO/AIMD-97-79	VETSNET experienced schedule delays and missed deadlines because (1) it employed a new software development language not previously used by the development team, one that was inconsistent with the agency's other systems development efforts; (2) the department's software development capability was immature and it had lost critical systems control and quality assurance personnel, and (3) VBA lacked a complete systems architecture; for example, neither a security architecture nor performance characteristics had been defined for the project.
September 15, 1997 GAO/AIMD-97-154	VBA's software development capability remained ad hoc and chaotic, subjecting the agency to continuing risk of cost overruns, poor quality software, and schedule delays in software development.
May 11, 2000 GAO/T-AIMD-00-74	$11 million had reportedly been spent on VETSNET C&P; neither the May 1998 completion date nor the revised completion date of December 1998 were met. Contributing factors included lack of an integrated architecture defining the business processes, information flows and relationships, business requirements, and data descriptions, and VBA's immature software development capability.
September 21, 2000 GAO/T-AIMD-00-321	VBA's software development capability remained ad hoc and chaotic. The VETSNET implementation approach lacked key elements, including a strategy for data conversion and an integrated project plan and schedule incorporating all critical systems development areas. Further, data exchange issues had not been fully addressed.
April 4, 2001 GAO-01-550T	The project's viability was still a concern. It continued to lack an integrated project plan and schedule addressing all critical systems development areas, to be used as a means of determining what needs to be done and when. A pilot test of 10 original claims that did not require significant development work may not have been sufficient to demonstrate that the product was capable of working as intended in an organizationwide operational setting.
March 13, 2002 GAO-02-369T	VBA still had fundamental tasks to accomplish before it could successfully complete development and implementation. It still had to assess and validate users' requirements for the new system to ensure that business needs were met. It needed to complete testing of the system's functional business capability, as well as end-to-end testing to ensure that payments would be made accurately. Finally, it needed to establish an integrated project plan to guide its transition from the old to the new system.

Issuance date Report/testimony	Results of review
June 12, 2002 GAO-02-703	VA still needed to address long-standing concerns regarding development and implementation. VA needed to appoint a project manager, undertake a complete analysis of the initiative, and develop plans, including a revised C&P replacement system strategy and an integrated project plan. It also needed to develop and implement action plans to move VBA from the current to the replacement system and to ensure that the Benefits Delivery Network would be able to continue accurately processing benefits payments until the new system was deployed.
September 26, 2002 GAO-02-1054T	Much work remained before VBA could fully implement the VETSNET C&P system, and complete implementation was not expected until 2005. This meant that VBA had to continue relying on its aging Benefits Delivery Network to provide the more than 3.5 million payments that VA had to make to veterans each month. In late March, a VETSNET executive board and a project control board were established to provide decision support and oversee implementation, and VBA expected to hire a full-time project manager by the end of September. VBA also began revalidating functional business requirements for the new system, with completion planned by January 2003, and it identified actions needed to transition VBA from the current to the replacement system. VBA also hired a contractor and tasked the contractor with conducting functional, integration, and linkage testing, as well as software quality assurance for each release of the system applications. Despite these actions, completing implementation of the new system could take several years. All but one of the software applications for the new system still needed to be fully deployed or developed. Specifically, a rating board automation tool (RBA 2000) was deployed, although VBA did not plan to require all its regional offices to use it until July 2003. In addition, two others had not been completely deployed: one of these (Share, used to establish a new claim) was in use by only 6 of the 57 regional offices. The other (Modern Award Processing–Development, used to develop information on claims) was in pilot testing at two regional offices—Salt Lake and Little Rock—but was not expected to be implemented at the other 55 regional offices until October 2003. The remaining three software applications (Award Processing, Finance and Accounting System, and Correspondence) were still in development.

Source: GAO.

(310769)

United States Government Accountability Office
Washington, DC 20548

July 24, 2006

The Honorable Shelley Berkley
Ranking Member
Subcommittee on Disability Assistance and Memorial Affairs
Committee on Veterans' Affairs
House of Representatives

The Honorable Stephanie Herseth
Ranking Member
Subcommittee on Economic Opportunity
Committee on Veterans' Affairs
House of Representatives

Subject: *Veterans Affairs: Subcommittees Post-Hearing Questions Concerning Appropriate Policies and Audit Controls at Veterans Benefits Administration.*

This letter responds to your June 29, 2006, letter containing questions relating to our testimony on June 20, 2006.[1] At that hearing, we discussed the information security program of the Veterans Benefits Administration and the Department of Veterans Affairs, including weaknesses reported by us and others, as well as actions that the department has taken to address past recommendations. We also discussed potential measures that federal agencies can take to help limit the likelihood of personal information being compromised, and we identified key benefits and challenges associated with effectively notifying the public about security breaches. The questions from Ranking Member Berkley and Congressman Udall, along with our responses, are attached. In preparing these responses, we relied on federal guidance and our previous work in this area.

We are sending copies of this letter and attachments to the Secretary of Veterans Affairs. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Key contributors to this correspondence include Charles Vrabel, William Cook, Valerie Hopkins, Jeanne Sung, and Jeffrey Woodward.

Gregory C. Wilshusen
Director, Information Security Issues

Attachments (2)

[1]GAO, *Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs*, GAO-06-897T (Washington, D.C.: June 20, 2006).

Attachment 1: Questions from Ranking Member Berkley

1. *Please describe what audit requirement policies, such as logging and monitoring, should be in place to assure the integrity of VBA data.*

To help ensure the integrity of their data, organizations should collect and maintain audit trails on their information systems that are sufficient to log security-relevant information. Audit and monitoring technologies can help security administrators to determine what, when, and by whom specific actions were taken on a system; routinely assess computer security; perform investigations during and after an attack or data breach; and even recognize an ongoing attack.

In its special publications on computer security,[2] the National Institute of Standards and Technology (NIST) recommends that audit logs record the following information for each system event:

- the type of event and its result, including failed user authentication attempts, changes to users' security information, and organization- and application-specific security-relevant events;
- the date and time of the event;
- the user identification associated with the event; and
- the program or command used to initiate the event.

NIST also recommends that audit trails be protected from unauthorized access and retained for a sufficient period of time; system managers and administrators should consult with the organization's computer security personnel to determine how long audit files should be retained.

Organizations should use automated audit analysis tools to distill the most relevant information from raw audit data as well as to help reduce the amount of information contained in audit records. Because the volume of security information that must be reviewed is often very large, the most effective monitoring efforts are those that target specific actions, such as unsuccessful attempts to gain entry to a system or access sensitive information, deviations from access trends, successful attempts to access sensitive data and resources, and use of highly sensitive access privileges.

Organizations should also monitor system activity by regularly examining and reviewing audit trails. These reviews can be conducted periodically, as needed upon occurrence of a security event, automatically in real time, or in some combination thereof. Personnel who review audit trails should have a sufficient understanding of system activity so that they can effectively identify unusual or inappropriate activity. In addition, organizations should investigate and review audit trails following known system or software problems, known user violations of security policies, or system or user problems for which no explanation exists. Furthermore, to provide secure storage for logs and improve their incident handling capability, organizations should

---

[2]National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, SP 800-12 (Gaithersburg, Md.: October 1995); and *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14 (Gaithersburg, Md.: September 1996).

deploy centralized logging servers and configure logging devices throughout the organization to send duplicates of their log entries to the centralized logging servers.

2. *Please indicate what level of staffing is needed to effectively provide independent audit review of software development in an agency the size of the VA.*

The level of staffing needed to conduct an independent audit review of software development at agencies such as VA depends upon several factors. These factors include the characteristics of the system or systems being reviewed, the objectives and scope of the review, and the knowledge, skills, and abilities that reviewers need in order to conduct the review.

The size and complexity of the information systems and software being developed and the nature and extent of the agency's software development activities will influence the level of staffing needed. For example, reviewers should consider the extent to which software is purchased as commercial off-the-shelf (COTS), acquired as COTS and then modified, custom developed by agency staff, custom developed by contractor staff, or developed using some combination thereof. Reviewers also need to consider the number and magnitude of systems that are being developed and the types of computer processing to be performed (stand alone, distributed, or networked) by the systems under development, including the type and extent of system interfaces with other information systems.

The objectives and scope of the review also affect the level of staffing needed to review software development activities. The objectives and scope are influenced by, for example, the number and size of the systems being reviewed, the portions of the software development life cycle being reviewed, and assessment of the risks affecting the review. For example, a review could encompass individual elements of the development life cycle, such as requirements definition, system testing, or risk management or it could address the entire development life cycle. In general, as the number and size of systems increase and the scope of the review increases, the level of staff needed to conduct the review increases.

The knowledge, skills, and abilities of the independent reviewers can affect the level of staffing. Such knowledge, skills, and abilities include:

- knowledge of federal guidelines for designing controls into systems during development;
- knowledge of the procedures, tools, and techniques that provide control over application software development and modification;
- knowledge of the risks associated with the development and modification of application software; and
- ability to analyze and evaluate the entity's methodology and procedures for system development and modification and identify the strengths and weaknesses.

By assessing these factors, independent reviewers can determine the appropriate level of staffing necessary to achieve the objectives of the review and provide appropriate oversight.

Attachment 2: Question from Congressman Udall

1. *GAO identified weakness in segregation of duties and change control at the Austin Automation Center, but did not evaluate these issues at the Hines and Philadelphia VBA data centers. Can you describe examples of the kinds of segregation of duties and audit controls that these offices should have in place?*

Federal agencies should segregate incompatible duties and establish audit controls that safeguard programs and data in order to reduce the risk that errors or fraud will occur and go undetected. Incompatible duties that should be separated include application and system programming, quality assurance, computer operations, and data security. The following are examples of restrictions that are generally addressed in policies about segregating duties and can be achieved through organizational divisions and access controls.

- Application users should not have access to operating system or application software.
- Only users, not computer staff, should be responsible for originating or correcting transactions and for initiating changes to application files.
- Computer operators should not have access to program libraries or data files.
- Programmers should not be responsible for moving programs into production or have access to production libraries or data.

In addition, steps involved in processing a transaction also need to be separated among different individuals. For example, the following combinations of functions should not be performed by a single individual:

- data entry and verification of data,
- data entry and its reconciliation to output,
- input of transactions for incompatible processing functions (e.g., entering purchase orders, receiving information, and vendor invoices), and
- data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds a pre-defined limit requiring a supervisor's review and approval).

The VA Office of Inspector General recently reported that it has continued to find security vulnerabilities related to the lack of segregation of duties at VA facilities.[3]

Changes to the operating system software should be documented, authorized, tested, independently reviewed, and implemented by a third party in order to ensure that the changes are needed, work as intended, and do not result in the loss of data and program integrity. Federal agencies should have a documented system development life cycle methodology that details the procedures that are to be followed when applications are being designed and developed, as well as when they are subsequently modified. The following are examples of topics that are generally addressed in policies about change controls:

---

[3]Department of Veterans Affairs Office of Inspector General, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, No. 06-02238-163 (Washington D.C. 20420: July 11, 2006).

Attachment 2: Question from Congressman Udall

- Detailed information about who can authorize a modification and how authorizations are to be documented.
- A disciplined process for testing and approving new and modified programs before implementation to make sure that programs operate as intended and that no unauthorized changes are introduced.
- Established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who will use it.
- Maintenance of copies of approved software programs in carefully controlled libraries to ensure that they are protected from unauthorized changes or impairment and that different versions are not misidentified.
- Clear policies regarding the use of personal and public domain software by employees at work.

(310581)