HEARING ON THE REPEATED FAILURES OF VA'S INFORMATION TECHNOLOGY MANAGEMENT

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

June 14, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-51

28-127.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

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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*

CONTENTS

June 14, 2006

	Page
Repeated Failures of VA's Information Technology Management	1

OPENING STATEMENTS

Chairman Buyer	1
Hon. Bob Filner, Ranking Democratic Member	3
Hon. Michael Michaud	5
Hon. Jeff Miller, prepared statement of	34

WITNESSES

Staley, Michel L., Assistant Inspector General for Auditing, Office of Inspector General, U.S. Department of Veterans Affairs	7
Prepared statement of Mr. Staley	36
Koontz, Linda D., Director, Information Management Issues, and Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office	8
Prepared statement of Linda Koontz and Gregory Wilshusen	46

HEARING ON THE REPEATED FAILURES OF VA'S INFORMATION TECHNOLOGY MANAGEMENT

Wednesday, June 14, 2006
U.S. House of Representatives,
Committee on Veterans' Affairs,
Washington, D.C.

The committee met, pursuant to call, at 10:34 a.m., in Room 334, Cannon House Office Building, Hon. Steve Buyer [chairman of the committee] presiding.

Present: Representatives Buyer, Moran, Miller, Brown of South Carolina, Boozman, Bilirakis, Filner, Michaud, Herseth, Snyder, Salazar, Udall and Reyes.

The Chairman. The House Committee on Veterans' Affairs will come to order. Today is June 14, 2006.

Good morning, ladies and gentlemen. We are here today to receive testimony from the Department of Veterans Affairs Inspector General and the Government Accounting Office about past problems and recommendations in connection with information security and management at the VA.

We are on a fast track here at the committee. With the security of personnel data compromised last month and the very trust of veterans and their families at stake, we cannot afford to let time pass. Already we have held one hearing to learn about the immediate impact of the theft from the Secretary last week, joined by the Military Quality of Life and Veterans' Affairs Appropriations Subcommittee Chairman, Jim Walsh; and I have held a roundtable at which information technology experts from Goldman Sachs & Company, EMC Corporation, VISA, Citi Group, Tri-West, and the American Bankers Association offered very candid appraisals, all emphasizing the importance of a centralized management of key components of information and information systems.

Today, we must establish how and why the second largest breach of personal data in American history occurred at the VA. Then, continuing an aggressive series of hearings over the next 2 weeks, we will hear testimony from experts, largely from the private sector and the academic world, which will provide best practices to further guide us.

Finally, we will be hearing also from the VA General Counsel, Tim McClain, with an update on the progress being made at the Department as well as the legal ramifications of this breach. We will then hear again from Secretary Jim Nicholson at the end of the month.

We must identify and understand the scope of this problem. Then we can determine how to correct the problems at the Department. We will then act on that determination.

Today is essentially about the past, about context. Without the advantage of this historical context, the theft of an analyst's computer might appear to be an aberration, something unusual that can be corrected with a new policy or an official rule.

The context shows something entirely different. VA's internal controls and data security have been grossly inadequate for years. Both the VA IG and the GAO have indicated VA's decentralized management and the lack of accountability as major shortcomings which have led to 16 recurring, unmitigated information security vulnerabilities over the past 8 years.

Since May of 2000, this committee has held six hearings where VA information security has been specifically addressed and where lapses have been repeatedly identified. We have continued to hold three more hearings this Congress to review VA information technology and monitor the Department's actions with respect to IG and GAO recommendations and even directives from Department leadership. In the upcoming hearings, we will continue to obtain insights from witnesses, which will help us develop a bipartisan approach to this problem.

The next hearing will be on June 20, when the Subcommittee on Disability Assistance and Memorial Affairs and the Subcommittee on Economic Opportunities will hold a joint hearing on the VA data theft and cyber security procedures at the Veterans Benefits Administration. This hearing will include an examination of security measures to ensure fiduciaries are protecting sensitive client information.

On June 21, the Subcommittee on Health will be meeting to examine the Department of Veterans Affairs efforts to maintain security and integrity of the electronic health records of enrolled veterans while safeguarding sensitive personal veteran information from internal and external security threats.

On June 22, the full committee will meet to hear from academic and industry experts on operational aspects of IT security, as well as the VA General Counsel on legal implications.

On June 28, we will examine the role of VA's Chief Information Officer and the Department's Office of Information and Technology Structure and Operations. We will receive testimony from two of the former CIOs at the VA.

And, finally, on June 29, we will bring back VA Secretary Jim Nicholson to testify before the full committee to provide us with an update of the status of the VA data theft.

Please make sure, my colleagues, that you mark these important dates on your schedules. To the extent that information security is a critical priority throughout government, what we hear today and the successive hearings on this issue will, I believe, be of a broad value that transcends any one agency.

I now recognize Mr. Filner for an opening statement.

MR. FILNER. Thank you, Mr. Chairman.

You used the words "aggressive" and "fast track" in these series of hearings, and I certainly appreciate that, and we will give you our full support. I think you have mapped out a fine approach from this committee, and we thank you.

If it were possible to approach the theft of veterans' and service members' records without the emotions triggered by this theft, and what I can only call a pathetic response from the Veterans' Administration, the emotions of disbelief, anger, frustration that we all feel, this situation might be even an interesting case study of lax policies, failed leadership, and organizational arrogance. I can only call this situation the Katrina of the Veterans' Administration. A disaster occurred presumably not of their own doing, and yet the response was clearly inadequate, causing more suffering, and a presidential crony at the top of the administration unable to respond in an adequate way. I know that Mr. Nicholson doesn't want to hear this phrase from President Bush, that he is doing a heck of a job.

We have 26.5 million veterans and over 2.2 million active and reserve service members at risk of identity theft, their lives now requiring a new and constant vigilance. Sensitive disability codes pinpointing health and medical information on service-connected disabled veterans, their most private personal information, is poised to enter the public domain, with the steady drip, drip, drip of information each time adding more bad news. A lot of sensitive information is involved here, with a baseless spin by Secretary Nicholson and the other VA officials that the stolen data, and I quote, "may have been erased by teenagers who sold the computer equipment."

Reaching for outcomes that are less than tragic is not helpful in this situation, when the street value of this information probably exceeds half a billion dollars, quite an incentive for bad guys to get ahold of this data.

We are collectively angered by the 19-day-long lag between the data theft and public announcement. When we questioned what happened, we find that the employee who took the data home told his supervisors almost immediately about the theft, but it took 6 days for the VA Chief of Staff to find out and another 6 days for the Deputy Chief of Staff, the Deputy Secretary, and the VA General Counsel to

get around to notifying the Secretary. Don't some of these folks work in the same office suite as the Secretary? Wouldn't it be reasonable to tell the boss immediately about the possibility of a great compromise of records?

Then we learn that the Inspector General's initial involvement was not a result of direct notification by the leadership at the VA but because someone from the IG's office happened to attend a regularly scheduled information security meeting. We have to question why the leadership of the VA would not be more proactive in getting the issue to the investigators at the IG.

In addition, it seems that the VA's senior leadership was more focusing on communicating with the White House than on notifying the FBI. That task fell on the IG. While the most important action should have been to recover the stolen data, message management was more important to these political appointees than getting the FBI involved in the investigation of the burglary. When the FBI was finally brought into the investigation, the trail was already 2 weeks old. Talk about misplaced priorities!

Not until this point did the VA Secretary notify the Nation's veterans, on May 22, fully 19 days after the theft.

The Secretary now clamors for stiffer penalties for government employees who mishandle personal information that is entrusted to them. Yet this organization failed to update in any meaningful way the internal policies and regulations of information security before the theft. VA just simply ignored a host of findings and recommendations over the years and never fixed any of the data control and information security problems; and, unbelievably, after the theft, the Secretary waited for over a month to implement an updated and substantive policy on information security. Even that policy is somewhat light on enforcement and on specific liabilities and punitive actions when an individual fails to protect sensitive information.

I believe, and I think the Chairman has said many times, this ID theft would not have happened if VA leaders since 2001 had cared about protecting sensitive data or could get the job done. This would not have happened if this Congress was more of a co-equal oversight mechanism for the executive branch. So we will learn today the history of information security and information technology problems at the VA, which the Chairman has amply outlined.

There still is avoidance of accountability and responsibility at the VA. One wayward employee alone did not give birth to this massive data compromise. It was born of a culture of indifference and fathered by VA leaders who philosophically skipped town during the last 5 years in their collective attempts to avoid accountability.

Anyone at VA who waited or delayed over 24 hours to report this compromise should be held accountable and fired. From the first day, it was clear this was not a minor issue. Likewise, anyone who inter-

fered, blocked or undercut the numerous attempts to improve substantive, enforceable information security and IT policies should be held accountable. I am looking forward to the testimony today to see how we may deal with that.

Lastly, Mr. Chairman, I spent the last days of May, and the early part of June, talking to people all over my district. Veterans were not only angry but scared. They have the potential compromise of their most sensitive data. They got a letter from the VA just recently, and they see a Web page from the VA, which says, basically go talk to your credit bureau.

The VA should be proactive in response to this crisis, making sure veterans know that the data breech will not be a cost to them, either in money or in psychological anxiety. We have an obligation, given what happened, to be comforting in every way possible, and the VA simply is not doing this. I hope over the course of your month-long hearings, Mr. Chairman, I think that the VA should sit down with the credit bureaus and ask them to voluntarily provide, as a national service, a way to mark these 26 or 28 million records so if any undue activity occurs we know about it right away, and it is not left up to the individual veterans to figure out how to deal with it.

My colleagues, Mr. Salazar and Ms. Hooley, have legislation which calls for monitoring of the credit reports; and also Mr. Salazar has recently introduced legislation for an ombudsman at the VA to begin to deal with this data breach.

Let us be proactive and not wait for more disasters to occur.

Thank you, Mr. Chairman.

THE CHAIRMAN. I thank the gentleman.

As far as I know, the committee, on a bipartisan basis, Mr. Filner, has gone back to 1997, according to GAO testimony, from their audit. That was in submitted testimony.

Does anyone have any other opening statements?

Mr. Michaud, you are recognized.

MR. MICHAUD. Thank you, Mr. Chairman.

Just briefly, I want to thank you for staying focused on this very important issue. I commend you and Ranking Member Evans for your leadership and having the committee explore this fully with an aggressive schedule over the next month. I really appreciate it.

I also want to thank Congressman Salazar for introducing legislation to look at this issue.

I look forward to hearing the witnesses testify here today, and I would ask that my opening statement be submitted fully for the record.

THE CHAIRMAN. All written statements will be submitted for the record, and members will have 3 business days to do so.

[No statement was submitted.]

[A statement for the record of Jeff Miller appears on p. 34.]

THE CHAIRMAN. Any other opening statements?

All right, we will go to the witnesses.

Today, we welcome Michael Staley, the Assistant Inspector General for Audit at the Department of Veterans Affairs. Mr. Staley served with the Second Battalion Ninth Marines in Vietnam in 1968. Upon returning from Vietnam, he devoted his career to helping veterans and their beneficiaries. He held several positions of responsibility at the Veterans Benefit Administration upon joining them in 1971.

Michael Staley was appointed the Assistant Inspector General for Auditing in December of 2003. He directs a nationwide staff of over 185 auditors and support staff located in offices across the Nation. His office conducts audits and evaluations of the Department of Veterans Affairs programs and functions and provides audit support to criminal and administrative investigations.

Also before us is Ms. Linda Koontz. You have been before us quite often over the years, and we appreciate your testimony. She is the Director of Information Management Issues at the U.S. Government Accounting Office.

We also have Gregory Wilshusen, Director of Information Security Issues at the U.S. Government Accountability Office.

Ms. Koontz is responsible for government-wide telecommunications issues as well as issues concerning the collection, use, and dissemination of government information in an era of rapidly changing technology.

Mr. Wilshusen has over 22 years of auditing and financial management information technology management experience and is the acting director on GAO's information technology team, where he leads information security audits at several Federal agencies.

We also have Mr. Raponi with the VA IG; and I will leave that, Mr. Staley, for any further introductions.

STATEMENTS OF MICHAEL L. STALEY, ASSISTANT INSPECTOR GENERAL FOR AUDIT, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY MICHAEL RAPONI, REGION DIRECTOR, ST. PETERSBURG AUDIT OPERATION DIVISION, U.S. DEPARTMENT OF VETERANS AFFAIRS; LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; AND GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

THE CHAIRMAN. Mr. Staley, you are now recognized.

STATEMENT OF MICHAEL STALEY

MR. STALEY. Thank you, Mr. Chairman.

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

As you said, Mr. Mike Raponi is next to me today. He served as the project manager on the IT security audits, as well as I have Steven Gaskell in the audience, who also served as a project manager on these 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. As such, we have included IT security as a major management challenge for the Department in all of the major management challenge reports since the year 2000.

In our annual financial statement audits, we have reported VA information security controls as a material weakness since our fiscal year 1997 audit. Specifically, we reported that VA's financial data and sensitive veteran medical and benefits 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 to achieve standardization, remediation of identified weaknesses, and accountability in VA information security. We have continued to report control weaknesses in physical security, electronic security, reporting, wireless security and employee security. Additionally, we have reported significant issues with the implementation of IT initiatives by VA.

Our combined assessment program reviews continue to report physical security and access control security vulnerabilities at VA health care facilities and VA regional offices where security issues were evaluated. We have recently issued an advance copy of our draft IT security program review to VA. 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 testimony.

In closing, I would like the committee to know that reviews of VA's information security will remain a top priority in my office. We remain committed to reporting on the adequacy of IT information security controls and following up on actions taken by VA to strengthen

these controls as we remain dedicated to the goal of protecting our Nation's veterans.

Mr. Chairman and members of the committee, thank you for the opportunity to be before you today; and I would be pleased to answer any questions that you might have.

[The statement of Michael Staley appears on p. 36.]

THE CHAIRMAN. Ms. Koontz, you are recognized.

STATEMENT OF LINDA KOONTZ

MS. KOONTZ. Mr. Chairman and members of the committee, thank you for inviting us to participate in today's hearing on information security and privacy at the Department of Veterans Affairs.

The recent well-publicized security breach of the Department has thrown into high relief the importance of good information security controls in protecting personally identifiable information, not only at VA but throughout the government. As we have reported many times, poor information security is a widespread problem that can potentially have devastating consequences.

Today, we would like to summarize the recurring security weaknesses that we have reported at VA, discuss what agencies can do to prevent breaches of personal information, and comment on the issue of notifying individuals and the public when breaches occur.

Since 1998, GAO and the VA IG have reported on wide-ranging deficiencies in VA's information security, including the lack of effective controls to prevent unauthorized access to VA systems and sensitive data. In addition, the Department had not consistently provided adequate physical security for its computer facilities; it had not assigned duties so that incompatible functions were segregated; it had not controlled changes to its operating systems; and it had not updated or tested its disaster recovery plans.

These deficiencies happened at least in part because VA had not fully implemented key components of a comprehensive, integrated information security program. Such a program would establish Department-wide policies and procedures to address these weaknesses.

Further, as we reported in 2002, VA's organization and management may also have hindered its ability to fully address security challenges. Specifically, we reported that the hundreds of information security officers in VA did not report either directly or indirectly to the cyber security officer, and this official did not have control over a significant portion of the financial resources that the security program depends on to sustain its operations.

VA has taken steps to improve information security. For example, it reports that it recently centralized its security management. However, 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.

In addition to a robust security program, agencies, including VA, can take a number of steps to help guard against the inadvertent compromise of personally identifiable information. Specifically, under the E-Government Act, agencies are required to conduct privacy impact assessments. Going forward, this gives agencies the opportunity to assess upfront how personally identifiable information is to be collected, stored, shared, and managed so that controls can be built in from the beginning.

In addition, we suggest that agencies can take a number of other practical steps. They can limit the collection of information to what they really need, they can limit the time that they keep such information, they can limit access to that information and train personnel accordingly, and they can appropriately use technological controls such as encryption when data needs to be stored on portable devices.

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, notifications to those affected or the public has clear benefits, allowing people the opportunity to protect themselves from identity theft.

Further, although existing law does not require agencies to notify the public, 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 protections.

That said, we need to be careful to define appropriate criteria for triggering notification, and notices must be sufficiently informative to allow people to understand the threat and how they should respond to it. As the Comptroller General testified last week, these are factors we think that Congress should consider as it deliberates on proposed legislation on breached notification.

In summary, Mr. Chairman, 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, its efforts have been insufficient to address these serious issues. Only through strong leadership and sustained management commitment can VA implement a comprehensive, integrated information security program that can effectively manage risks on an ongoing basis.

Mr. Chairman, that concludes my statement. Mr. Wilshusen and I would be happy to answer questions.

THE CHAIRMAN. Thank you very much.

[The statement of Linda Koontz and Gregory Wilshusen appears on p. 46.]

THE CHAIRMAN. When I think about the lapses of security in some of the hearings we have had over the years we had some problems in pension compensation fraud. So whether it was a $12 million case in Atlanta, a $6 million case in Manhattan, a $6 million case at Bay Pines, each time we come up here we talk about what the problems were; and it always goes back to unauthorized access, not having sufficient controls, who had the keys, where was the authority. I hate to keep saying it, but it is ditto, ditto, ditto. It is almost like you can prepare your testimony by looking back on the testimony that you have given over the years.

So here is what is sort of exhaustive. You highlight these problems and concerns not only from GAO but IG, and you hand these off to the administration. Who acts on them? Who is supposed to act on the reports?

MR. WILSHUSEN. Well, at least with regard to the GAO reports, we usually direct our recommendations to the head of the agency, and then they may direct it down to lower levels of management.

THE CHAIRMAN. And in this case it is the Secretary?

MR. WILSHUSEN. In this case, it would be to the Secretary of VA. Because, under FISMA, which is the Federal Information Security Management Act, it is the head of the agency that is responsible for implementing the safeguards and information security controls necessary to protect the information and information systems under his control that support the operations and assets of that agency.

THE CHAIRMAN. All right. Mr. Staley? I mean, you provided testimony from your fiscal year 2004 report, including 16 recommendations, all of which remain open as of today. So these reports go to whom?

MR. STALEY. We issue our draft reports, Mr. Chairman, to the Chief Information Officer; and our recommendations in this report that you referred to included the Chief Information Officer and all of VA senior leadership that was involved in any IT security functions so that they could act jointly in trying to resolve these 16 recommendations.

In our prior reports, we have issued our reports to the Chief Information Officer; and his concern and his response has been that he doesn't have the enforcement authority to implement the recommendations solely by himself. So, in an attempt to remediate that issue, we were then broadening our recommendations to include all of VA senior leadership.

THE CHAIRMAN. All right, but -- okay, so when you are faced with a general counsel's decision that the CIO could only go with compliance and not enforcement, you then would take your reports and send them to whom above the CIO? When you say "senior management," I don't know what that means.

MR. STALEY. If we are unable to resolve a recommendation or to get an action plan that is acceptable, we would then elevate it to the

Deputy Secretary and the Secretary, if necessary.

THE CHAIRMAN. Where does the CIO obtain his authority?

MR. STALEY. The CIO obtains his authority from the FISMA act.

THE CHAIRMAN. Does he not also obtain his authority from directives from the Secretary?

MR. STALEY. Certainly, he is responsible to reporting to the Secretary, and he is under his leadership.

MR. WILSHUSEN. And, also, if I may add, Mr. Chairman, Mr. Staley is correct. FISMA, in addition to making -- having the Secretary assume overall responsibility for the program, he also can delegate to the CIO the authority to ensure compliance with the Act and the provisions of the Act and to develop and maintain an agency-wide information security program that contains several different elements including assessing risks, developing the policies and procedures that are necessary to reduce those risks or cost-effectively reduce those risks, and to provide the testing and evaluation regarding the compliance and effectiveness of those controls.

THE CHAIRMAN. I have one last question. Are you aware -- Ms. Koontz, are you aware of the memorandum of March 16, 2004, whereby then Secretary Tony Principi made an effort to make sure that cyber security, accountability,and protecting VA's computer information systems was the responsibility of the CIO Robert McFarland?

MS. KOONTZ. Yes.

THE CHAIRMAN. You are familiar with that memorandum?

MS. KOONTZ. I have read it. Yes.

THE CHAIRMAN. Are you also familiar then with the general counsel's opinion that said that, despite the Secretary extending authority, that he really did not have the authority of enforcement? Are you familiar with the general counsel's memorandum?

MS. KOONTZ. The general counsel memorandum that I am familiar with is from February, 2004. I don't know if this is the same one or not. I am not sure I have all the documentation that you have, but a similar issue was raised at that time.

THE CHAIRMAN. I have one here dated April 7, 2004. So I will make sure you get a copy of this.

MS. KOONTZ. Okay. Very good.

THE CHAIRMAN. My question is, is when you look at the FISMA legislation that we passed here in Congress, were there rulings from other general counsels of other government departments consistent to what the VA did with regard to authority of a CIO?

MS. KOONTZ. We haven't done a government-wide review of that, but I am not aware of any other general counsel that has -- any other counsel decisions that would be similar.

MR. WILSHUSEN. Nor am I.

THE CHAIRMAN. You are not aware of up to date, but you have not given it a review.

MS. KOONTZ. I haven't done a systematic review, no, and asked everybody.

MR. CHAIRMAN. Would you be outside of your lane to do that for this committee?

MS. KOONTZ. I don't think so.

MR. WILSHUSEN. No, we could work with your staff to look at that.

THE CHAIRMAN. All right. What we are most curious about is whether this legal opinion is consistent with other general counsels' opinion of the interpretation of the Act, or was this an opinion that was written because it was placating toward the interests of the three Under Secretaries?

MS. KOONTZ. I understand.

THE CHAIRMAN. Mr. Filner, you are recognized.

MR. FILNER. Thank you, Mr. Chairman.

It is a bit beyond the scope of your testimony, but I would like to know if either of you have thought about or would need further direction from this committee to think about a proactive response. That is, we have an unprecedented breach of security here. I know personally that dealing with identity theft is extremely difficult, it is frustrating, it is time consuming. People who are older especially, find it hard to fix. They need our help.

Have you thought about a way that we can, in fact, taking into account privacy concerns, give the veterans some help from us, rather than leave it to them as individuals to figure out credit breaches or monitor their credit reports or get their credit reports? Could the VA figure out a way to work with the credit bureaus to monitor any suspicious activity, and therefore know of problems immediately? To put some of the burden on the VA rather than on the individual veteran? Can you comment? Have you thought about that at all?

We have to think outside the box, as they say. We are thinking in very traditional terms about dealing with this issue, and yet this massive breach and the kind of people that we have a responsibility to deserve better.

MS. KOONTZ. There are probably a number of options that are available to the Congress to deal with this if the Congress makes a policy decision that this kind of action is warranted. I have seen proposals all the way from offering veterans free credit reports over some period of time to working more proactively with the credit bureaus in terms of monitoring. But, quite honestly, we haven't evaluated any of these proposals nor looked into it further.

MR. FILNER. Are you restricted to evaluating?

MS. KOONTZ. Yes.

MR. FILNER. We have to have some people giving us some policy recommendations in response to this breech, not just an audit function.

THE CHAIRMAN. Mr. Filner, that is what we have done in our coordination of hearings. We will have academics, we have private in-

dustries and all. We have brought in the auditors for them to give us the historical context of all the problems and concerns. When we understand the context of the problem, then we can move out toward a solution.

MR. FILNER. I appreciate that, Mr. Chairman.

An independent audit that was done about a little more than 3 years ago -- this was not done by either GAO or IG but Deloitte and Touche -- and I quote from that report. In the so-called C and P system, compensation and pension, we identified numerous security weaknesses, including inappropriate access privileges and inadequate management of access privilege, excessive assignment of powerful privileges to sensitive information, and inadequate segregation of duties, permitting individuals to both initiate claims and authorize the claims for disbursement.

It seems to me we knew that there was a disaster waiting to occur. Do you have any comment on that? Is that part of what you had found in previous years?

MR. STALEY. Well, in commenting to the report, sir, the report continued to talk about role-based user profiles in terms of --

MR. FILNER. I am sorry. Can you define this in English, please?

MR. STALEY. Identifying the employee's specific duties, and then identifying what specific data that employee would need to perform those duties, and then limiting the access and controlling the access to only that specific set of data. What we are finding is that there is a broader set of data that employees are able to access.

By going ahead and limiting that access and I think, as Ms. Koontz has said in her testimony, by going ahead and restricting how much they can get, you certainly can mitigate the risks of some employee going off farther into other data than they should be.

MR. WILSHUSEN. I would just add that those lists of deficiencies that you just pointed out from the Deloitte report are very similar -- in fact, identical -- to many of the weaknesses we identified years before then, after from 1997 or 1998 to 2002. And I think it is just emblematic of the lack of having a comprehensive security program.

Because you can find problems and weaknesses on one system with one organization, and if you don't have a centralization of your controls and standardization you will end up finding weaknesses across the Department. Without having a strong, centralized focal point for implementing information security, it is likely that once an identified weakness is known it may be corrected, and VA generally is pretty good at correcting identified weaknesses, but they are not that good at proactively going forward and looking to see if similar weaknesses exist across the Department and taking corrective action.

MR. FILNER. Mr. Chairman, I don't mean this in any partisan way. I don't care if it is a Democratic administration or a Republican Congress or vice versa or executive-legislative being in the hands of the

same party. The oversight function of Congress is critical. You have shown, as we look down the month's schedule, the proper way to do oversight. I think all the committees have to take this more seriously, again, without any partisan thought. I think you have outlined a way that a committee ought to do oversight, and I hope we can serve as an example for other committees, too.

My time is up. Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you. Mr. Moran.

MR. MORAN. Thank you, Mr. Chairman.

We have heard for a long time, and you have outlined again today, a long list, a long history of weaknesses within the system. My interest is perhaps beyond your realm of ability to answer, but how do you explain the failure of the VA to implement the recommendations and for the atmosphere or culture that exists at the VA in regard to this issue to continue despite the significant and series of warnings that have occurred over a long period of time? What is wrong at the VA that inadequate response occurs, it seems to me, in each and every occasion to the Inspector General, to the GAO, and to congressional committees' direction following review of their procedures? Why no or insufficient response?

MR. STALEY. One of the reasons I think, sir, is that the recommendations -- the Department has seemed to focus on a resolution of recommendations at the sites that we visit. We go out to the information technology centers, and then we go out to a select number of medical centers or regional offices, and then we conduct these program reviews where we go out to offices. And the responses we get back to those recommendations are, is we have taken actions at site A.

Then next year we come along and we go to site B and we see that the same conditions exist. We have been continuing to report that these are systemic issues and that you need a comprehensive and central approach to ensuring that all of the recommendations are issued at all the sites concurrently. So we wind up going ahead and making the recommendation the following year, and so then it just seems to perpetuate itself.

Really, the Department needs to take an aggressive stance in ensuring that all of the regional offices and all of the facilities are correcting the vulnerabilities that we have identified and also correcting the vulnerabilities that they have recognized through their own certification and accreditation process in order to mitigate the risks that we are talking about here today.

MR. WILSHUSEN. If I may add, because I wholeheartedly endorse what Mr. Staley said, is also there needs to be appropriate accountability mechanisms in place to help assure compliance; and, if not, that there are consequences for not implementing security controls.

MR. MORAN. Mr. Wilshusen, your testimony was that, legally, the responsibility for these issues, the security of information contained

at the VA, rests with the Secretary of the Department. Is that true?

MR. WILSHUSEN. Yes, under the Federal Information Security Management Act.

MR. MORAN. So no question as to who is responsible legally.

MR. WILSHUSEN. He has overall responsibility.

MR. MORAN. What is your reaction to what is very troublesome to me as about the time frame in which it -- the time passage. Say that differently. A long period of time -- at least in my mind, a long period of time transpired before this breach reached the desk of the Secretary, and yet you tell me that the Secretary is legally responsible for this system and the consequences of that breach. What does it tell us about the VA in the failure for this information to quickly reach the Secretary?

MR. WILSHUSEN. One of the elements that is required under law by FISMA is that agencies develop the policies and procedures for adequately detecting, reporting, and responding to security incidents and events.

It seems clear -- and, again, we haven't done any work, so I don't know the specifics of this other than what I have read -- but it seems like there might have been a breakdown in those policies and procedures.

MR. MORAN. Are there policies for response and for notification in place at the VA today?

MR. WILSHUSEN. That is something we haven't looked at recently.

MR. STALEY. There is an incident response criteria in VA's handbook. We currently have an administrative investigation ongoing to look at the specific instructions of the incident response handbook and what occurred from the point of time where the employee notified the VA. We hope to issue that report to the Department for comment at the end of this month; and as soon as the Department responds to our issues and recommendations, we will be issuing the report, hopefully in mid-July.

MR. MORAN. Well, as I indicated, this aspect of it is clearly troublesome to me, the idea that it would take so long for the Secretary to learn of this breach. The concern it raises with me is we either have a desire at a level of the VA in which to camouflage or hide, cover up the errors and mistakes, or a suggestion that the Secretary or the upper management is disengaged in these issues. And either one is a terrible conclusion to reach.

But I would like to know -- I am anxious for your report, Mr. Staley -- to learn why it would take such an extraordinary amount of time. I just know in the management of any business, small or large, the first place you go with something of this magnitude is to the leader; and it clearly happened in a very slow fashion at the Department of Veterans Affairs.

Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you very much. Mr. Michaud.

MR. MICHAUD. Thank you very much, Mr. Chairman.

Question: During the coordinated draft, VA directive 6500 information security program, VHA questioned the requirement that all companies acting as contractors or subcontractors with access to VA's information system, including transcription services and medical devices, shall be American owned.

Today, the VA Office of Inspector General will release a report indicating that, in February of 2005, an offshore subcontractor contacted the Office of Inspector General hot line division threatening to expose about 30,000 VHA patient records from five VHA facilities over the Internet if the contractor did not pay over $28,000 owed. Draft directive 6500 would have prevented this. But the culture within VHA, as explained at previous hearings, that "don't tell me what to do" attitude, questioned the American-owned transcription service requirement. They went out, but, as a result, confidentiality of medical records of over 30,000 veterans was jeopardized.

I would like you to comment.

MR. STALEY. Yes, sir. We have been conducting this audit for some time in conjunction with our Office of Investigations, because there have also been certain investigations that have been ongoing as well, some of which would been under seal, so we have been a bit delayed in issuing this report. In fact, we worked with the Justice Department a few months ago to try to sort out what language we could or could not put in the report before we issued it, and we just recently received comments back from the Justice Department.

The break in the control is that the contracts do not specify to the contractors a number of criteria in terms of how to protect personal identifying information. Such as you can send it to a U.S. contractor, but you cannot use an offshore foreign subcontractor. It is silent on the issue. So, consequently, you have an issue such as you have described this morning arise.

And, of course, our report hopes to be out on the Internet today, latest tomorrow; and it talks about four issues: using speech recognition technology in-house to try to keep more of this in-house and not outsource it because the information is so sensitive; acquiring transcription services uniformly; and verifying the invoices and then, most importantly, the management controls over patient privacy and personal patient identifiers.

THE CHAIRMAN. Mr. Michaud, if the gentleman would yield to me. I recognized you out of order, and if you hold your thoughts, let me recognize Dr. Snyder, because he is going to have to get to the Armed Services Committee.

MR. MICHAUD. No problem.

THE CHAIRMAN. Mr. Snyder.

MR. SNYDER. Thank you, Mr. Chairman. I appreciate your holding

this hearing, also.

I don't know if it happened to you, Mr. Chairman, but, as I mentioned in another hearing, my wife and I have a 3-week-old baby, so we got about 3 weeks behind in our mail. Two days ago we were going through literally a laundry basket full of mail because we are on so many lists, and there was my letter from Secretary Nicholson, and I thought I was not going to be -- did you think the same thing?

THE CHAIRMAN. It was personalized, too.

MR. SNYDER. It was very personalized.

THE CHAIRMAN. "Dear Veteran."

MR. SNYDER. It gives you this empty feeling when you realize that somebody is sitting out there with your stuff.

But at one of the hearings that was held, I think it was in the May 25th hearing -- I will direct this to you, Mr. Staley -- some private-sector privacy experts suggested that the VA doesn't need to be using Social Security numbers at all; and, in fact, that we were all -- everybody in the military memorizes for all time their service number. We could either use our service number, which is just distinctly for the military, or be assigned another number. Why do we have to use a Social Security number at all since this is all an in-house thing?

MR. STALEY. Well, it is certainly a policy decision by the Department. But my views on that, as I had a service number and not a Social Security number, but I also joined the VA around 1971, so I recognized that the Department of Defense was moving from service numbers to Social Security numbers depending on the branch of service you were in. So VA eventually moved Social Security numbers as your general identifier. And many of your affiliations and your other business associates that work with the VA also use Social Security numbers. Department of Defense uses Social Security numbers. So I think that is pretty much how Social Security numbers became the --

MR. SNYDER. I understand why it was done 35 years ago. But why do we perpetuate it? We have a distinctive number that is not a Social Security number. Would that not add a different level of protection if we got away from Social Security numbers?

MR. STALEY. Certainly your point is well taken.

MR. SNYDER. They go throughout their military career with using a number that is not their Social Security number. Is that not correct?

MR. STALEY. I am sorry, your question again?

MR. SNYDER. People in the military go throughout their military career, whether it is 2 years or 20 years, with a number that is not their Social Security number as their identifying number. Is that not correct?

MR. STALEY. I believe -- I am not sure whether all military branches use a unique service number. I couldn't comment on that.

MR. SNYDER. I want to get back to Mr. Buyer's statement about this memorandum on the CIO authority. And I haven't read this, I just quickly looked through it.

When you start seeing -- when someone has to ask for this kind of guidance and somebody is quoting court cases on statutory authority, you know, the principles of interpreting statute, we are in doo-doo city. I mean, because somebody out there has to sit -- is looking for how do I have to do my dang job? And do I have authority or not? And when I call up you to tell you I have the authority, I don't need to be sending along: Well, you need to refer to page 7, footnote 3, about my authority to tell you how to improve your stuff. I mean, does this not point that we need to do some clarifying legislative kind of language so that the lines of authority on this are clear?

MR. STALEY. Obviously, I can't speak for the general counsel in that their legal opinion has been the focal point of the reasons why the CIO has continued to inform us, as we push forward in trying to move our recommendations forward, that he had been hampered by enforcing many of the initiatives that he had tried to execute in terms of having the authority to make them happen.

MR. SNYDER. And you folks from the GAO, there is a statement in there. You talk about the weaknesses, that things have been identified in 2001 that had not been resolved, what Mr. Buyer referred to as the ditto document, that we are rehashing some of the stuff had been talked about in the past. In one line there in the report, it talks about the Department has maximized limited resources to make significant improvements. The phrase "limited resources" catches my attention. Do we have now and have we had funding issues in terms of getting this done?

MR. WILSHUSEN. I think that was the Department's response.

MR. SNYDER. It was the Department's response. Do you agree with that response? Is it partly a money issue?

MR. WILSHUSEN. We believe -- and in our reports we talk about what resources are available that they have and how they are being used. I wouldn't say that is a resource issue or that they need more money. We generally don't make such recommendations along those lines. We look at how they use the resources that they have.

MR. SNYDER. Dr. Staley, one of the problems that you mentioned is controlling access to physical space. Now we can talk about encryption and all these kind of things as being a new problem. We all understand new problems. But access, protection of medical records, physical space is not a new challenge. Why is that not an easy problem to correct?

I assume what we are talking about is the ability of someone just to walk in and say I am going to grab that file. Why are we still having to deal, after this many decades of concern about medical privacy, before even the advent of computers, why are we still dealing with

controlling access to physical space, just somebody walking in and grabbing files?

MR. STALEY. Well, it is an issue of vigilance, sir, and continually ensuring that your physical space is secure. Obviously, the Department has made improvements by adding key cards and things of that nature to control physical space better. We see more and more of that as we go out on these site visits.

But it doesn't preclude someone from sticking a pop bottle in that door, and then we arrive and, my goodness, there is a pop bottle and the door is open. It doesn't preclude cleaning crews from going in there unescorted, or because of a lack of time, someone lets a contractor in there to deliver materials and they are not there next to them.

So these physical security issues continue to persist, and it is really an issue of vigilance and ensuring that our guard is not let down and that those areas are always secured.

MR. SNYDER. If you see in your work, if you see Mr. Buyer's or my file laying around, would you let us know?

Thank you. Thank you, Mr. Chairman.

THE CHAIRMAN. Dr. Snyder, your question with regard to Social Security numbers. At the last hearing, Gartner Consulting gave a recommendation to the committee that the VA should no longer use Social Security numbers and should use a user personal identifier. So, distinctive.

Your other question on enforcement, where we are going, is the reason we have turned now to the other subcommittees to hold their own hearings. Because if the CIO can't do the enforcement, then the enforcement is the responsibility of the three Under Secretaries. So we have got to bring them in.

MR. SNYDER. Thank you.

THE CHAIRMAN. Mr. Michaud.

MR. MICHAUD. Thank you very much, Mr. Chairman.

I just want to follow up on my last question. St our last hearing we were assured that there is a culture within VHA based upon the medical profession code to do no harm by Dr. Perlin. But my concern when I find out that just last year that you received a call from a subcontractor threatening to expose 30,000 veterans' information, medical records, over the Internet unless VA pay the $28,000 owed is a real concern that I have. And I am just wondering, in your many reviews of the VA IT system, have you identified a stronger IT security culture in VHA versus the Veterans Benefits Administration or the National Cemetery Administration?

MR. STALEY. Our principal focus is in the Veterans' Health Administration and the Veterans' Benefits Administration. They have far more platforms and systems than the National Cemetery Administration. There is only a few systems that are being used there. And we are finding similar problems in both administrations. Referring

to encryption solutions, you will find the same problems, that the veterans' benefits network does transmit clear text, unencrypted among its network. You go to VHA, you look at their Vista system, which is predominant, and the transmission and storage is in clear text. And when you look at some of the other areas that I have testified on in my written testimony, similar conditions exist in both administrations.

MR. MICHAUD. Has the GAO found that with other agencies dealing with subcontractors, that this is a problem? Have you looked at this issue as a potential problem?

MR. WILSHUSEN. We looked at the issue last year in terms of the use of contractors to provide services, information technology and security-related services; and one of the things we found is that Federal agencies, by and large, did not do an adequate job of providing oversight over the services that those contractors provide.

One of the things -- again, I keep referring to FISMA. But one of the things that FISMA does, is it also extends the requirement that the agency's information security program extends to the information and the systems that are being operated on its behalf by contractors and other third parties; and we found that there is still room for improvement on agencies' oversight of the work being done by contractors with regard to information security.

MR. MICHAUD. Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you.

Mr. Bilirakis.

MR. BILIRAKIS. Thank you, Mr. Chairman.

Mr. Staley, as you may know, tomorrow the Subcommittee on Oversight Investigations will hold a hearing on patient safety, where we will hear testimony from GAO on credentialing physicians, which includes background checks, of course. Your written testimony states that you have identified instances where background investigations and reinvestigations were not initiated in a timely manner on employees and contractors or were not initiated at all. Now, are you telling this committee that the Department is lacking background checks for personnel that handle secure data as well?

MR. STALEY. Yes, Mr. Bilirakis.

MR. BILIRAKIS. You are saying that.

MR. STALEY. Yes. VBA has recently reported to our office that they need to conduct about 3,000 new background checks in order to resolve this issue. So that is one of the reasons our recommendation remains open and why we continue to monitor it.

MR. BILIRAKIS. My God. We identified IT and security deficiencies at 37; 67 percent of 55 Veterans' Benefits Administration facilities reviewed. And this is something that has been in the offing, as you know, for a long, long time. We have held hearing after hearing after hearing. We have had roundtables. We can just go on and on and

on.

I guess we can continue to talk about the details here and about Social Security numbers, but I don't know why in the world we got away from the old military service numbers, quite frankly, and went into Social Security numbers. All we did was just compounded the problem.

Mr. Moran went into the atmosphere of the culture. I would add an additional word to that, and that is turf, T-U-R-F. Frankly, one of my biggest disappointments -- and I am not a spring chicken. I have served in the military. You just name it. Basically, I think I have done it all. Yet it is still one of my biggest disappointments since coming to the Congress 24 years ago is the turf concerns that we have up here. I think we probably would function one hell of a lot better if we weren't as concerned with it as we are. And maybe it is human nature and maybe it is something we can't ever change because it is within us. I don't know. But that is a terrible disappointment on my part.

I might add, too, my first experience with the IG was when I was in the military, and I saw a lot of power there. I mean, people straightened up and paid attention when the IG got involved in a particular situation. Now we have GAO which -- thank God for you. I think, frankly, you do great work. And we have the IG. And yet we haven't been able to straighten things out at the VA.

Granted, we have secretaries who are political appointments, many of whom don't even serve the full 4 years that they are appointed. I think that there is a lot of resentment probably towards them by the bureaucrats.

Why can't we get these things straightened out? I mean, don't you have any recommendations to us? Is the only way to get this culture and this atmosphere that exists there and these turf problems -- and I know you haven't acknowledged that yet, but I think you probably would acknowledge that turf is part of the problem. Isn't there any way to get this straightened out without necessarily someone coming in and saying just we are going to clean out everybody? And I don't want the papers to report that I have suggested that, but -- clean out everyone and start from scratch? Why should we continue to -- I mean, it creates work for us and whatnot. And maybe that is good, because we are needed. But, at the same time, why can't we get past that?

Comments? GAO, Ms. Koontz, say you are queen of the day. I mean, tell me, what would you do?

Ms. Koontz. Well, I think one of the things that I didn't want to leave this hearing without saying is that one of the very serious problems at VA has been the lack of a strong CIO organization, and VA was very slow to put into place a full-time CIO. That didn't happen until 2001. And, since then, there has been two CIOs who have come

and gone. Each of them recognized that there was a need to realign the CIO function and to strengthen it.

We supported the notion that you needed to have centralized security management, and we supported the idea that the CIO really had to have a seat at the table and needed to have veto authority, power over things that just didn't make sense, that weren't standard within the organization, that shouldn't be connected to the network, that didn't meet security standards. And what you have seen is that two CIOs have come and gone and the realignment has yet to happen.

Obviously, VA is very, very resistant to change, quite slow to move. And I have to say I think it is up to the Secretary to make sure that the CIO has the support to make the realignment happen in such a way that we can get a positive result.

MR. BILIRAKIS. Should that CIO be someone coming through the ranks, so to speak, a bureaucrat, or should it be somebody from the outside?

MS. KOONTZ. I think that the CIO has to have particular qualifications, and the CIO at VA is a political appointment. I think that the talent and the qualifications of the person is probably most important, but, also, the support from the Secretary is very vital.

MR. BILIRAKIS. But if that CIO is and has to be -- I mean, I don't know whether that person has to be a political appointment. But if he or she has to be a political appointment, won't that person maybe suffer the same problems that the Secretary -- any Secretary might because of resentment and the culture that exists there and this is an outsider coming in?

MS. KOONTZ. I think that will be a challenge for anyone coming up, either within the ranks or from outside. And, again, I think that the Secretary has the authority and the power to make sure that the CIO can be effective in the organization, even though I recognize there are big challenges in terms of all the reasons that you have just mentioned -- that it is a very large organization, it is very difficult to change, and there appears to be some resistance to changing things in this area.

MR. BILIRAKIS. In the process -- and I don't see the red light on yet, Mr. Chairman, so I guess I will continue. But in the process of your investigations and also the investigations of the IG, you go into the details and you see things wrong and you make recommendations, but do you take into consideration this culture, invisible type of thing, culture, turf, atmosphere type thing in the process? Or do you just concentrate on, I will say, the tangible, if you will, the mistakes that are made, the inefficiencies, and things of that nature?

MS. KOONTZ. Well, I think -- from a GAO perspective, I think we always try to identify what the root cause is of any particular deficiencies that we found. And I think we have reported over and over that -- management being a very critical problem at VA in terms of

IT and one that needs to be resolved. So I think we have taken that into consideration.

MR. BILIRAKIS. Mr. Staley, anything to add on that? Again, I said my experience with you all is that you are awfully powerful, but are you not powerful as far as the VA is concerned.

MR. STALEY. We continue to make recommendations, Mr. Bilirakis. In my written testimony, the first recommendation speaks to a centralized approach which we recognized because each administration needs to work together to resolve the vulnerabilities that are talked about in the testimony from 2 to 17, in that all of the administrations need to work together to achieve success. And I know there are some very hardworking individuals in each of the administrations that have specific missions for their specific administration. But there is a bigger picture here, in that what everything points to is a standardized approach, and the only way that can be accomplished is if it is all done as one voice.

MR. BILIRAKIS. Do you see continuity? Secretary Principi left, Secretary Nicholson came aboard. I guess there was probably a little bit of a gap period of time there. Is there continuity? How much time is spent by those two secretaries, along with their chief personnel, to sit down and to kind of go over, hey, this is what has been a problem, this is what we have accomplished, this is what we have kind of turned over to you and recommend? Is that taking place?

MR. STALEY. In the case of Secretary Principi he was very adamant that the administrations complete their certifications and accreditation process by August 21, 2005. And he made that happen. And it also allowed the Department to realize and to catalog the number of vulnerabilities that it really had to deal with just by the fact that they were able to certify and accreditate all of their systems. It also gave them a better handle on how many systems they really had. So Secretary Principi did make progress in that area, of course; then he had moved on. And now we have secretary Nicholson trying to get a handle on this issue.

MR. BILIRAKIS. Thank you.

THE CHAIRMAN. We will have a second round. Ms. Herseth.

MS. HERSETH. Thank you, Mr. Chairman. If I could make just a request to add on to yours, in working with the committee and with the GAO to undertake a systematic analysis of the general counsel's rulings. I would alsoinquire, Mr. Chairman, as to your willingness to extend that to look at, in light of Ms. Koontz's acknowledgment or her explanation of what she thinks is a problem here and a lack of a strong CIO organization, we have got since 1996 under the Klinger-Cohen Act, a CIO is supposed to be created in each Federal agency. It would be interesting to see if we have the same problem in the other Federal agencies with the lack of a strong organization with the CIO, if there are other determinations, and maybe we can extend it.

I only bring it up because we need some continuity across agencies. And if they are having the same problem in another agency with the lack of a strong CIO that has led to some of the same problems that the VA has been experiencing based on a currently decentralized system but the need for some sort of centralization, we have other CIOs that have been created in other Federal agencies. And I do not know if they all communicate effectively about the different problems they are having, but we do need to facilitate the exchange of information among these different entities we create after statutory authority to do so.

THE CHAIRMAN. Your point is well taken. The reason we focus on this memo, and we will bring the general counsel up, is that Tony Principi, the former Secretary, went out and found one of the Nation's best and brightest in Bob McFarland to be the CIO to take on these challenges that GAO and IG have laid out. But what happened is we had a strong intelligent person who is undercut in his authority to be able to implement it, and that is what we are going to get to the bottom of.

I yield back.

MS. HERSETH. I appreciate that, Mr. Chairman, and I hope that we can pursue this in other ways because I think -- and this leads to sort of my next question here -- if we can identify where things are working better in a different agency with a new position that we create, that way it helps us to identify how we improve, kind of find sort of the best practices for other agencies.

So that leads me, Mr. Stalely, to my question for you. And that is on page 3 of your written testimony, and I know that Mr. Bilirakis identified this as well. We have a number, significant percentages here of our VHA and VBA facilities that have an ongoing problem with implementing recommendations and have these vulnerabilities. But has there ever been an analysis as to what is going right or what steps were taken at the 40 VHA facilities and the 18 VBA facilities in which these comprehensive reviews have shown that the recommendations were acted on or they have been able to avoid or take corrective action to address the vulnerabilities so that as we seek to centralize and standardize the procedures, is it differences in leadership at the regional offices? Is it differences in attitude? We have all posed questions about culture. Is it differences how resources are being allocated?

I would rather us move -- while we can talk for hours about the problems, maybe we could shift our focus to those sites, those facilities, that have done a good job, and figure out how we integrate their practices into our desire to have a more centralized and effective system to address the vulnerabilities. Has a similar analysis and trying to figure out and put together a best practices has been completed?

MR. STALEY. Certainly we haven't reported as a cumulative on best

practices, as you have suggested. It is a good point. What we have done is discuss a best practice or a control in an individual report. But no, we have not taken those facilities that are complying and are vigilant about access controls and those kind of issues and talked about them as; here is a body of work and here is what you need to do for example. We haven't done that.

We have reached out to these PCIE communities. My IG has reached out to the PCIE to talk about whether we need to get together as a group and look at this issue governmentwide. I do know that we are scheduled to meet with the PCIE in the future and talk about this very issue.

MS. HERSETH. And the acronym stands for what again? Did you say PCAI?

MR. STALEY. PCIE, the President's Council on Integrity and Efficiency.

MS. HERSETH. That was going to be another question. That is the entity that brings all the offices of the inspector general together.

MR. STALEY. Yes.

MS. HERSETH. To identify patterns and trends. And how often does that Council get together?

MR. STALEY. It is routine. I cannot give you an exact time but usually monthly.

mMs. Herseth. Just as a follow-up, Ms. Koontz, are you aware at the GAO, do the CIOs created among the different agencies, do they have a mechanism in which they get together on a regular basis to share information?

MS. KOONTZ. The CIOs also have the CIO Council which was established -- or reestablished under the E-Government Act.

MS. HERSETH. So they all meet together. They are meeting in sort of subsets of one another, based on whether they are in the IG office or CIO?

MS. KOONTZ. Right.

MS. HERSETH. I will yield back. I hate to end on this note but I think it is important to put this on the record again because it is an observation that has some pretty powerful implications. In the first hearing that we had on the data theft, we secured a written statement from Dr. Leon Kappelman who is an expert in information technology in our organization, culture, and operations. Here is what he observed. He has personally seen VA personnel subvert and sabotage hundreds of millions of dollars' worth of IT projects and read about billions more wasted on other failures. I have seen a total disregard for one cyber security effort after another. These are only the tip of the iceberg.

Why do such things happen at VA? Largely because these systems and efforts would make the utilization of budget and personnel more transparent and thereby make accountability possible. Have either

of you in your work ever seen evidence at different facilities of personnel intentionally subverting and sabotaging projects designed to implement recommendations, particularly in the cyber security and information technology arena?

MR. WILSHUSEN. No, I cannot say that I have seen any personnel sabotaging such projects.

MR. STALEY. The same for me. I can not recall any specific instances. Of course we are an audit organization. We do have an Office of Investigations, but I cannot speak for any specific instance where that may have occurred.

MS. HERSETH. I appreciate your responses.

MR. BILIRAKIS. Will the gentlewoman yield.

MS. HERSETH. Yes, Mr. Bilirakis.

MR. BILIRAKIS. As a follow up on that, how does the VA in your opinions, particularly GAO because you have experience throughout all of the other departments and agencies, how does the VA compare in these areas with the other departments and agencies?

MR. WILSHUSEN. At least with regard to information security, every year we look at the FISMA reports that are required that each agency is supposed to send to the Congress and also to OMB. Our analysis of those FISMA reports tends to show that VA and its implementation of the FISMA requirements tends to be at the bottom end of the scale, if you will, along with some of the other larger, more diverse organizations compared to other smaller organizations that tend to do higher on that particular score. But certainly with VA reporting material weaknesses since 1998, 1997, it is an indication that there is a lot of work that needs to be done.

MR. BILIRAKIS. Thank you.

THE CHAIRMAN. Thank you very much. I would like to go to your issue number one and it deals with the implementation of a centralized agencywide IT security program. We got to go to this one because a lot of people will -- and it is easy to say this is the responsibility of the CIO. Really? I suppose that is what it should be in corporate America and it is. It is what it should be at the VA but it is not.

So Tony Principi goes out there and he finds one of the best, makes him the CIO, and then we learn that operational controls are decentralized among each of the administrations; so VHA, VBA, the National Cemetery Administration and other programs, they have the operational control. The CIO can only provide guidance and the tools to support these activities but has no ability to enforce. Is that statement correct?

MR. STALEY. That is correct. Correct, sir. That is correct, sir.

THE CHAIRMAN. I wanted to make sure I was hearing correctly. That is an important predicate. It is an important predicate because we need to figure out what are the lines of authority. If you figure out what are the lines of authority, then we can get to the implementa-

tion to cure the problem.

In Congress when we looked at this last year on a bipartisan basis, we moved overwhelmingly, not only in this committee but in the entire House. Not a single vote against centralizing the IT system. Whoa, did we get pushed back. The Senate wanted to give deference to the VA and the bureaucracy became the centurians. Wow. Then we continued to receive your reports about all of these issues that are still noncompliant. I suppose, then, if we have a system that is so decentralized -- but let's go back.

We have the Secretary who has the authority. He then extends part of his authority to CIO and part of that goes to cyber security, both of which can only do compliance but not enforcement; therefore, I must assume that enforcement then rests with the three Under Secretaries. Would that be a correct assumption?

MR. STALEY. That is correct.

THE CHAIRMAN. So it is now the responsibility of the three Under Secretaries to implement these recommendations from GAO and IG; would that be correct? I am looking for responsibility, Mr. Stalely.

MR. STALEY. The CIO in conjunction with VA leadership, they have a joint responsibility to implement these recommendations. That is correct Mr. Chairman.

THE CHAIRMAN. Okay. Both of you have an incredibly challenging job. When you see something in error and you keep highlighting the error and you are trying to work with someone else who says, I know all about it but I have no authority, and this has been happening for years.

Let me ask this. On GAO you have got to have a higher authority. If the GAO turns to the VA and for years you give these recommendations to cure, yet you have a department of government that is not implementing GAO recommendations, who is your higher authority?

MR. WILSHUSEN. I would just say, you know, it is the management's responsibility for implementing those recommendations. We continue to make them.

THE CHAIRMAN. Who is the manager of the management?

MR. WILSHUSEN. That would be at the agency. It would be the Secretary and the senior managers of CIO, as others.

THE CHAIRMAN. Wait a minute, wait a minute. I do not understand the answer. At the GAO you are overlooking departments of government, and you have a department of government that is noncompliant and perhaps even recalcitrant from a bureaucracy that will not implement the changes, who do you appeal to. Do you turn to OMB? Do you report this to the White House? Is there a higher appellate authority? Or do you just say, you know what, the Secretary reports to the Cabinet and all we can do is we're auditors. We can tell them what we see and if they act on the information that is great; if they do not act, well, I guess that is what happens.

MR. WILSHUSEN. Well, we do report to the Department; that is correct. I do not know if we would appeal to OMB on a specific instance where a department is noncompliant with implementing our recommendations.

THE CHAIRMAN. So your audits would only go to a Secretariat of a department, and they do not go anywhere else.

MR. WILSHUSEN. No, we also send, usually, copies of the recommendations; and our reports go to different congressional committees of jurisdiction.

THE CHAIRMAN. So outside of our oversight and the Senate's oversight, what oversight is there in the executive branch if you have a department of government that does not implement changes to prevent a train wreck? I don't know. If there is not, just tell me. I am not asking you a question I know the answer to. I do not know.

MR. WILSHUSEN. I guess the only other higher authority might be the American public, because many of our reports are also publicized and put on the Web site.

THE CHAIRMAN. I will stay within the executive branch. Within GAO is there ever a function whereby you take your report and you send it to anyone else? The anyone else would be what? The White House. Because the Secretariats work for the President.

MR. WILSHUSEN. Generally, when we would do a governmentwide review, our recommendations and report would then usually be addressed to the director of OMB if it has OMB issues in it. But that would not necessarily be the result of our work that we have been doing over at VA.

THE CHAIRMAN. If it has OMB issues on it. All right. Let's go with theft, fraud, 6 million, right, 6 million, 12 million, these Bay Pines debacles, hundreds of millions of dollars. That is kind of OMB implication, right? So if you have got the VA nonimplementation, was there ever a thought within GAO that, gee, we probably need to kick this over to OMB? I am just curious. I do not know.

MS. KOONTZ. I think one of the mechanisms that we use is that we have publicized information security as being a governmentwide high-risk area since 1997, I believe. And we have put a lot of emphasis on it and there have been a lot of conversations with OMB and with the individual agencies about trying to address this particular weakness.

MR. WILSHUSEN. Right. And one other comment, too, is that agencies are to report how they have implemented the GAO recommendations. So I guess it is to the GAO oversight committees, which would be the House Government Reform and Senate Homeland Security, Government Affairs.

THE CHAIRMAN. All right. Let's go to Government Reform, because they ended up coming with the FISMA act. So we put teeth in Privacy Act violations. Are there sufficient -- is there sufficient teeth for

compliance in this act? Do you think Congress needs to come back in to the FISMA and make them equate with the Privacy Act violation?

MR. WILSHUSEN. I do not think there are any particular, I will say, penalties.

THE CHAIRMAN. Enforcement mechanisms? Tools?

MR. WILSHUSEN. Right. Other than agencies are required to report to Congress and to OMB on the progress of implementing FISMA.

THE CHAIRMAN. And there are no consequences for not?

MR. WILSHUSEN. For not reporting? I do not know if that has happened. I think each agency has reported.

THE CHAIRMAN. Ms. Koontz, I can remember the first time in your testimony before one of the subcommittees that I chaired, the VA was the last to go out and get a CIO that I recall. It was driving me crazy with the Klinger Act. And that is when I first -- I had deep respect for you because you went right at it. And our difficulty right now is that we have so many of these security vulnerabilities, key controls, information that should have never been taken down, information that does not even -- if you have an individual that gains access to particular information, it is not even time sensitive.

This is going to take a tremendous amount of work to put this one together. Does anybody else have further questions? Mr. Moran.

MR. MORAN. No, sir.

THE CHAIRMAN. Mr. Bilirakis.

MR. BILIRAKIS. I guess you have to go over there.

MR. MICHAUD. Yes. Thank you, Mr. Chairman. FISMA applies to national and nonnational security systems. The data that was stolen, does that fall in that category as national or nonnational security?

MR. STALEY. Sir, I am really not able to comment at this time, in that we currently have an ongoing administrative investigation and we are also doing a set of comprehensive policy reviews as well and working with the Justice Department. And I believe our intention is to get that report out at the end of the month to the Department for comment, and then to issue it to the public and to the Hill by mid-July.

MR. MICHAUD. So you cannot comment whether it was national or nonnational?

MR. STALEY. I would not be able to comment -- sir.

MR. MICHAUD. Assuming that it was or is a national or nonnational -- assuming that it was or it is -- my question is that on August 1 of 2003, the general counsel issued an advisory opinion to address the extent of the authority and responsibility to the VA chief information officer contemplated by the Federal Information Security Management Act of 2003 as a national security information and information system. It held that FISMA charges the CIO with certain security responsibilities, a major one being the development and maintenance of information security policy, procedures and controlled techniques

to ensure security requirements issued by the President and OMB requiring national and nonnational security systems are met. FISMA requires the CIO to develop and implement an agencywide security program to achieve these purposes. Has this happened? Why or why not?

MR. STALEY. Certainly. Our reports have repeatedly shown that security vulnerabilities continue to exist in many facets of the Department, and that the VA even itself reported itself as receiving an F grade in terms of IT security. I think, as GAO had pointed out, they have a long way to go to mitigate these vulnerabilities and to have a sound comprehensive IT security program.

MR. MICHAUD. When will you know whether or not this is a national or nonnational security issue?

MR. STALEY. Well, our report will be issued mid-July and it is conducting a comprehensive review of policy procedures and these other issues.

MR. MICHAUD. Thank you, Mr. Chairman.

THE CHAIRMAN. Mr. Filner.

MR. FILNER. I thank the panel for being here. I want to make two quick comments, Mr. Chairman. We can go through all of this analysis (we used to call it "analysis paralysis") and recommendations. Between the lines of the bureaucratese and the big words everybody is using, there is a failure of management at the very top. The Secretary has not taken control, and we should hold him accountable. It is as simple as that, as far as I can tell.

Secondly, it has been 6 weeks since this theft of data. The Department of Veterans Affairs finally got out a letter to people who were impacted by this theft, although they said they didn't get a letter out earlier because they did not have enough envelopes. The letter gives the veteran little support or help. The Web site that everybody has been referred to gives little or no help. The 800 number gives little or no help. Basically, the VA leaves it to the individual veteran to solve this massive issue.

It is about time that the VA had an answer for these veterans. We are going to make sure nothing happens again -- that we have centralized IT -- but we still have this problem. Veterans are not getting the help, and they better! I do not know how many people are sitting out there from the VA Department. They have a lot of people monitoring stuff rather than doing stuff. You better come back with a proactive stance soon. It has been 6 weeks. We should not go another week without having some help and hope for these veterans.

THE CHAIRMAN. Thank you, Mr. Bilirakis.

MR. BILIRAKIS. Thank you, Mr. Chairman. To get clear here -- and maybe we already are, I do not know -- the General Accountability Office used to be the General Accounting Office. So your responsibility is accountability. Is that accountability limited to just making

recommendations?

MR. WILSHUSEN. Well, we do follow up to see if they are taking corrective actions on our recommendations.

MR. BILIRAKIS. And if they haven't, that is it?

MR. WILSHUSEN. Well, we report on that.

MR. BILIRAKIS. You report on that.

MR. WILSHUSEN. Yes. We do not have the authority to actually implement the actions at the organizations.

MR. BILIRAKIS. So I guess it really gets back to, again, what we have been talking about here, not really knowing where the buck stops. And it really, I guess, stops with the head of the VA I, suppose, the head of the particular agency or department.

MR. WILSHUSEN. Well, under FISMA he is responsible for implementing appropriate safeguards.

MR. BILIRAKIS. Now, the IG sir, I keep coming back to you because I keep thinking that you have, or should have maybe, more authority. Again, in your case, what is it? You uncover things that go wrong and you make, what, you make recommendations, then?

MR. STALEY. Yes, sir. At the conclusion of our audits we make a series of recommendations to the Department. The leadership in the Department is responsible for implementing those recommendations. We have a follow-up system to determine whether their implementation plans are adequate and, again, if the recommendations are not implemented, we report them as such.

MR. BILIRAKIS. You report them to, again, going back.

MR. STALEY. They are in our semiannual report to Congress and to the Secretary. And we leave them open and we continue to ask the Department for corrective action.

MR. BILIRAKIS. Mr. Chairman, again, we can talk about details here, but I am not sure even -- we come up with legislation and we come up with laws and we mandate certain things and whatnot, but we are awfully busy people, despite the fact that we have oversight subcommittees. We are awfully busy people and we go off to maybe fight another fire or whatever the case might be. So it still comes down, I think, to culture and the mental state of the people who should be doing this job.

I do not really have any hope, I do not care how many hearings we hold, that any of that is going to change until the culture basically changes in the VA and the other organizations, here in this committee where our concern is the VA. It has always been my biggest concern ever since I have been in the Congress. It is disappointing. Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you, Mr. Bilirakis.

Ms. Koontz, I have to go back to the issue on GAO and what actions are taken when there is a Department that may not act. Have you ever seen any other Department or agency of government not act on

your recommendations with regard to IT?

MR. WILSHUSEN. Well, I would also just like to say with regard to VA, that on many of our recommendations that they have taken corrective actions, usually on the specific, detailed, technical control findings that we would identify. I do not want to leave the impression that they have not done anything. But with regard to the larger recommendations related to implementing an entitywide security program, their efforts have fallen short in that area.

Other agencies where we have conducted repeatable work, we find similar situations where we can make a number of detailed technical findings and recommendations. And often they will act on those, but it is more in terms of acting proactively and taking what they learned in terms of the identified findings and seeing if they exist elsewhere where they fall short. And again it often comes down to not having implemented an information security program agencywide. And, yes, those incidents do occur where we have made recommendations, and they have not yet fully implemented them.

THE CHAIRMAN. Tomorrow in the Commerce Committee under part of Mr. Bilirakis' leadership, along with Nathan Deal and Sherrod Brown, on a bipartisan basis, we are going to deal with the health record and the security of the health record and these kind of issues. We are going to create a position for a national coordinator within HHS so that we move toward more of a standardization with regard to plans and policies programmatics with the health record.

And so it is interesting. We are going to try to create that czar over the health record to make sure that everybody -- and we moved to centralized -- so here we are, Mr. Bilirakis and I, on the Commerce Committee, yet we are not going to defend a stovepipe. The stovepipe in this case would be our jurisdiction of the VA.

So when Mr. Bilirakis talks about the turf and everybody defending the turf, we are going to have to move toward the empowerment of this national coordinator to make sure it all gets implemented so we are not decentralized. So as we talk about centralized, what I see is that is the trend line, that is where everybody is going.

I asked staff, Ms. Koontz, to give up the August 1, 2003, memorandum from the general counsel that was read by Mr. Michaud. I give it to you because as you look at this question for us with regard to general counsel and the interpretation of the FISH bill, this is on August 1, 2003, they make a holding that is completely different than the April 2004. So it is almost like what happened over the year? So it will be interesting, the way to get into this. And we will be having Admiral Goss and Bob McFarland will both come in and give their testimony about what happened.

These were two individuals who were attempted to have been empowered, and then their authorities were taken away and we have

ended up with this mess. I think it is clear to the American people that this loss of data was not caused by just the negligent act of just one person. We have a systemwide meltdown of information management systems, and what we are going to do here in Congress is move a package that attempts to not only take actions to assist the veterans but also what can we do with regard to implementation down at VA?

I want to thank you for your leadership. We look forward to looking to your report. And, Ms. Koontz I have a feeling that you will be back before us soon. This hearing is now concluded.

[Whereupon, at 12:15 p.m., the committee was adjourned.]

APPENDIX

The Honorable Jeff Miller

Statement for the Record

June 14, 2006

As technology worldwide has improved to make our lives easier, it has also created new areas of concern that continually must be addressed. Among the foremost of these areas is the security of our personal information. Digital records abound through so much of our personal lives, including in commerce, the workplace, and interactions with government agencies.

Our nation is still reeling from the recent revelation of the potential compromise of a vast amount of personal information for our nation's veterans. Those who fought so bravely for our freedom so that we could rest at night should in

their personal information, including detailed records of their service, is secure.

It is my hope that today's hearing can give us an idea of how this could have been prevented as well as provide valuable insight to companies worldwide who are entrusted with valuable information such as individuals' social security numbers. I look forward to the testimony and to working with colleagues to be sure that our veterans are provided the appropriate recourse.

STATEMENT OF
MICHAEL L. STALEY
ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE
THE COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 14, 2006

INTRODUCTION

Mr. Chairman and Members of the Committee, 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 VA's implementation of OIG recommendations. I will provide an overview of the OIG reports that have shown the need for continued improvements in addressing information security weaknesses in VA and the status of OIG recommendations for corrective action.

SUMMARY OF PAST OIG REPORTS

We have conducted a number of audits and evaluations on information management security and information technology (IT) systems that have shown the need for continued improvements in addressing security weaknesses. We have reported VA information security controls as a material weakness in our annual Consolidated Financial Statements (CFS) audits since the fiscal year (FY) 1997 audit. Our Federal Information Security Management Act (FISMA) audits have identified significant information security vulnerabilities since FY 2001. We continue to report security weaknesses and vulnerabilities at VA health care facilities and VA regional offices where security issues were evaluated during our Combined Assessment Program (CAP) reviews. We have also included IT security as a major management challenge for the Department in all required major management challenges reports issued from FY 2000 to the present.

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 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 9, 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, the CAP program identified IT and security deficiencies in 141 (78 percent) of 181 Veterans Health Administration (VHA) facilities reviewed. We identified IT and security deficiencies at 37 (67 percent) of 55 Veterans Benefits Administration (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 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 was, until recently, vested with VHA, VBA, 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. 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 new sites visited 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 not previously visited in prior years 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. 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.

Issue 5: Background Investigations

VA 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 needs to validate whether VA completed installation of IDS at all 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.

Issue 8: Information Technology Centers' Continuity of Operations Plans

VA 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. 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 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. 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. Additionally, OCIS confirmed VHA has not completed the conversion of 161 older operating systems. In order to mitigate the risks associated with the

older operating systems, VHA moved the devices to a virtual local area network configuration with restricted access. 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. 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. 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, VA 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 vulnerabilities in the wireless network could be used to view transmissions, including those containing patient data, 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. VA was looking for solutions to establish controls to secure electronic protected health information. However, field tests conducted in FY 2005 continued to demonstrate the need to improve controls as our contractor's penetration test showed an intruder could successfully capture protected health information in unencrypted clear text from outside a VA network. Our site work also showed that unencrypted protected health information was vulnerable at other VHA facilities.

Issue 17: FISMA Reporting Database

FISMA establishes security requirements and requires VA to annually report vulnerabilities for systems and major applications. While VA 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 VA information and data at risk.

The FISMA database[1] contains the self-assessment surveys of VA'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 VA'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.

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. VA 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.

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

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 Committee 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.

Mr. Chairman and Members of the Committee 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 Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at time 10:30 a.m. EDT
June 14, 2006

VETERANS AFFAIRS

Leadership Needed to Address Information Security Weaknesses and Privacy Issues

Statement of Linda D. Koontz
Director, Information Management Issues

and

Gregory C. Wilshusen
Director, Information Security Issues

GAO-06-866T

June 14, 2006

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-866T, a testimony before the Committee on Veterans' Affairs, House of Representatives

VETERANS AFFAIRS

Leadership Needed to Address Information Security Weaknesses and Privacy Issues

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-06-866T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@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. Both GAO and the department's inspector general have reported recurring weaknesses 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.

Mr. Chairman and Members of the Committee:

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. 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.

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

[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.

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.

  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

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

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 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

[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).

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.

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

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.

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

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

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, 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

[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).

[26] GAO-06-421, pp. 59–61.

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 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 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

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

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 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

[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).

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, 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

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

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 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.

[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.

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;
- 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

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

- 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 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.

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

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 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.

[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).

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.

Mr. Chairman, 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.