UPDATE ON THE BREACH OF DATA SECURITY AT THE DEPARTMENT OF VETERANS AFFAIRS

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 29, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-59

28-455.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*
BRIAN BILLBRAY, *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 29, 2006

Update On The Breach Of Data Security at the Department of Veterans Affairs ..... Page 1

OPENING STATEMENTS

Chairman Buyer 1
Hon. Bob Filner 3
Hon. Cliff Stearns 4

STATEMENTS FOR THE RECORD

Hon. Corrine Brown 50
Hon. Tom Udall 55
Hon. John T. Salazar 56

WITNESSES

U.S. Department of Veterans Affairs:
Hon. R. James Nicholson, Secretary 5
Prepared statement of Hon. William F. Turek, Under Secretary for Memorial Affairs, National Cemetery Administration 58
Prepared statement of Hon. Jonathan B. Perlin, M.D., Ph.D., MSHA, FACP, Under Secretary for Health, Veterans Health Administration 67
Prepared statement of Hon. Gordon H. Mansfield, Deputy Secretary 76
Prepared statement of Hon. Ronald R. Aument, Deputy Under Secretary for Benefits, Veterans Benefits Administration 84

MATERIAL SUBMITTED FOR THE RECORD

Letter and Memorandum dated June 28, 2006, regarding Delegation of Authority for Responsibility for Departmental Information Security 98
VA Employee Home Use Amendment, Property Pass, and Justification for Access to SSNs, submitted by Mr. Filner 101

UPDATE ON THE BREACH OF DATA SECURITY AT THE DEPARTMENT OF VETERANS AFFAIRS

THURSDAY, JUNE 29, 2006

U.S. House of Representatives,
Committee on Veterans' Affairs,
Washington, D.C.

The Committee met, pursuant to call, at 10:30 a.m., in Room 334, Cannon House Office Building, Hon. Steve Buyer [Chairman of the Committee] presiding.

Present: Representatives Buyer, Stearns, Brown of South Carolina, Miller, Boozman, Bradley, Filner, Brown of Florida, Snyder, Michaud, Herseth, Berkley, Salazar.

The Chairman. The House Veterans Affairs Committee will come to order, June 29, 2006.

This morning we will continue our examination of the data theft and information security at the Department of Veterans Affairs. The catalyst of this examination was the compromise in May of data belonging to over 26 million veterans, 2.2 million servicemembers, and some family members. The purpose of our oversight has focused on obtaining as much understanding as possible, and has included business roundtable with information experts. We have had seven hearings including two Subcommittee hearings. This is nothing less than a full examination of the information management systems of the Department of Veterans Affairs.

What we learn here will inform us in our efforts to make whole any veteran harmed by the theft of personal information, and assure the security of veterans' personal information. Over the past month, this Committee has brought in over 17 witnesses to examine the loss of data, the current structure of information security as an extension of the structure of information technology, and options regarding credit monitoring and information security.

Witnesses have included Secretary Nicholson, the VA's Inspector General, General Counsel, experts from GAO, an academic; and experts in the field of data security, information technology management

and identity theft have testified. Additionally, the Subcommittee on disability assistance and memorial affairs held a joint hearing with the Subcommittee on economic opportunity on June 20th to review data security in the Veterans Benefits Administration. The Subcommittee on health held a hearing on June 21st to review the security of medical information in the Veterans Health Administration.

Today's hearing is a capstone event. Mr. Secretary, I want to thank you for being here this morning. We look forward to hearing what steps the department has taken to mitigate the second largest breach of personal data in American history, and how we are going to help our veterans. We are interested in learning as well what the VA is doing to prevent future security breaches, and what plans exist to mitigate the event of identity theft as a result of this breach or any other breach.

And before we receive your testimony, Mr. Secretary, in fairness to you, I offer a brief overview of what we have learned from these hearings, not to mention several years of painful experience in dealing with these issues and the VA's bureaucracy. Almost without exception, experts from academia and leading businesses have told this Committee that the complexities and threats characterizing information management today require the system to be centralized. They further state that the VA's decentralized IT structure make it, quote "practically impossible" end quote, to secure its data.

Time and again, we have heard the same counsel: limit the number of data users, minimize the amount of data that must be exported for use, screen and train your people, centralize the system, and empower the Chief Information Officer.

While no one knows whether this compromise of data will produce cases of fraud, executives who have successfully recovered from large-scale data compromises have informed this Committee that fast action is required. Communications with your customers is important when time is of the essence. Offer mitigating services quickly, and coordinate with law enforcement agencies quickly.

But the word "quick" does not seem to characterize anything about the VA's response to this threat over the years. The GAO and the department's own IG have testified on these issues repeatedly since 1997. They brought grave security deficiencies and vulnerabilities to the attention of VA officials, who in turn essentially have ignored them. Two immediate former department CIOs and a former associate deputy assistant secretary for cyber and information security informed this Committee of impenetrable barriers thrown up by a turf-bound culture of the status quo that affects your middle and senior ranks of leadership. The department's general counsel in 2004 I believe gave the narrowest possible interpretation of your predecessor's decision of his efforts to centralize IT authorities and empower the CIO.

Mr. Secretary, from this vantage point, I believe that at times you have not been well-served. You have inherited an unfortunate situation, and you are a military man yourself. I commend you on the acceptance of responsibility for a sorry state of affairs. But you are attempting to cut through the cultural resistance and fix it. I read the memo that you issued last night, and I congratulate you for that memo. I can almost envision the spirited debate that occurred at the table before you signed that memo, so I would like to thank you for that.

In your opening statement I would also, though, like for you to inform this Committee of any other data breaches that you have knowledge of; more in particular, the data loss in Minneapolis, and I am distressed to have heard about the lost tape in Indianapolis, because your counsel was just this week before this Committee, yet never informed this Committee that you have a missing tape that contains over 16,538 legal cases. So I am pretty stressed this morning to have learned this last night, very late.

At this point, I yield to Mr. Filner for any opening statement he may have.

MR. FILNER. Thank you, Mr. Chairman, and I again, as I have said in the preceding five hearings, thank you for this real example of oversight the Committee should be following.

Mr. Secretary, we are grateful about the announcement that you just made this morning. It lifts a heavy burden from the hearts of millions of veterans, if it is true that there was no compromise of the data. We congratulate law enforcement, and we can all breathe easier. I think everybody here is very grateful. But it doesn't change some fundamental things, Mr. Secretary. You start off with a little stunt, you never told us that the data had been recovered. Typical for this last two months, you have been spinning, spinning, spinning, you have been doing PR, and you have done very little to deal with the issue that the veterans face with fear every day.

It doesn't change the culture that we have had defined very clearly in these hearings, and which Mr. Buyer has been talking about for seven years. It doesn't change the lapses in your personnel chain, that has kept information apparently from you, from the FBI, and from us.

It doesn't change the fact that your intentions seem to be to have blamed all of this on one guy, who as we will show today at the hearing, had permission to take his laptop home, had permission to download the data, had help to download the data, had authorization to use that data, and yet he has been, as far as I know, the only one in your whole operation that any action has been taken against in a personnel way. He has been accused, as I understand, of gross negligence. But he did everything he was supposed to do. He informed his superior in 52 minutes. Your guys didn't inform you for six or seven

days. Who was grossly negligent?

So Mr. Secretary, we have got a lot to do. This memo that Mr. Buyer referred to is a good step. I agree on that. It is something that you, Mr. Chairman, have been working on for many years, and I know you feel some satisfaction in that. This theft, which hopefully has not compromised any identities, was the stimulus to take action. But the Chairman saw this coming for many years.

So we still must act. We still must act on the culture, we still must figure out why you decided to fire only one person in this whole mess, and whether he was actually grossly negligent, or other people were.

Mr. Chairman, I ask that my full statement be made part of the record.

THE CHAIRMAN. Hearing no objections, so ordered.

[No statement was submitted.]

THE CHAIRMAN. If any other members have opening statements, you may submit them for the record.

If you would like, I will yield to the gentleman.

[The statements of Ms. Corrine Brown, Mr. Tom Udall and Mr. John Salazar appear on p. 50, p. 55, and p. 56, respectively.]

MR. STEARNS. Mr. Chairman, I just want to commend the Secretary for his announcement this morning. I think it is breathtaking that he found the computer, and I commend he and his staff for doing it.

MR. FILNER. I don't think he found it.

MR. STEARNS. Well, at any rate, his announcement that at point they have the computer, and I think all of us are just waiting to hear more what has happened, and I think perhaps the angels are on his side at this point, so I will look forward to his comments.

MR. SNYDER. Mr. Chairman?

THE CHAIRMAN. Yes, Dr. Snyder.

MR. SNYDER. Thank you Mr. Chairman. I am not going to make a statement, but I was not here, and when I walked in— and so I hope the Secretary will begin anew, so I know exactly what Mr. Stearns is commending him for, thank you.

THE CHAIRMAN. We are going to give the Secretary great latitude, and we have invited him to come back after we had also done our due diligence and our investigations. And if you can recall, we had him here immediately after this happened, but also the Senate wanted him, so we only had him for about an hour. So we are going to have the Secretary here for as long as it takes this morning. And he has his under secretaries here, and Mr. Secretary, you are recognized.

STATEMENTS OF THE HON. R. JAMES NICHOLSON, SECRETARY, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY THE HON. GORDON H. MANSFIELD,

DEPUTY SECRETARY; THE HON. JONATHAN B. PERLIN, M.D. PH.D., MSHA, FACP, UNDER SECRETARY FOR HEALTH, VETERANS HEALTH ADMINISTRATION; THE HONORABLE RONALD R. AUMENT, DEPUTY UNDER SECRETARY FOR BENEFITS, VETERANS BENEFITS ADMINISTRATION; THE HONORABLE WILLIAM F. TUERK, UNDER SECRETARY FOR MEMORIAL AFFAIRS, NATIONAL CEMETERY ADMINISTRATION; THE HONORABLE TIM MCCLAIN, GENERAL COUNSEL, U.S. DEPARTMENT OF VETERANS AFFAIRS; JACK THOMPSON, DEPUTY GENERAL COUNSEL; THOMAS BOWMAN, CHIEF OF STAFF; DENNIS DUFFY, ACTING ASSISTANT SECRETARY FOR POLICY, PLANNING AND PREPAREDNESS; MARK WHITNEY, OFFICE OF POLICY, PLANNING AND PREPAREDNESS

SECRETARY NICHOLSON. Thank you, Mr. Chairman and members of the Committee. When I was coming in here I was asked if I would make a brief statement to the press because of the news that we have, the good news, and so I will start just by repeating that, by saying that it was confirmed to me by the Deputy Attorney General, just right before coming up here, that they have indeed, law enforcement has in their possession the subject laptop and hard drive; the serial numbers match.

We are diligently conducting forensic analysis on it to see if they can tell whether it has been duplicated, or utilized, or entered in any way, and that work is not complete. However, they did say to me that there is reason to be optimistic about that. But that is not a certainty.

I would like to again—I appreciate your kind words, Mr. Congressman. The only part I had in this recovery were my prayers to St. Anthony, I'll tell you. But the law enforcement community did a very, very good job in this. And to have, you know, gotten their hands on these two small items in the volume that there is circulating out there in that world is really extraordinary, and I am very grateful, and I know you are. We will just have to remain hopeful that they haven't been compromised, and as I said, there is reason to be optimistic.

THE CHAIRMAN. Are they studying the forensics right now?

SECRETARY NICHOLSON. As we speak, yes, sir.

THE CHAIRMAN. All right, thank you.

SECRETARY NICHOLSON. Again, I would like to thank you all for the opportunity to appear here today to follow up on what has occurred at our department. And my testimony, my opening statement will be in the context of this big problem, because I agree with Mr. Filner in many respects. This has brought to the light of day some real deficiencies in our department, and the manner in which we have

handled personal data and cyber information. And if there is a redeeming part of this, and I believe there is, is that we can really turn this place around, and I sincerely think we can make it into the gold standard for information security, like we have the gold standard for electronic health records. And that is our challenge, and indeed that is our mandate.

But I will testify in the context that things are as we thought they were last night, or yesterday at this time. So again, this theft occurred on May 3rd, and it has been tragic on many levels, but I also—and this may be moot, but there was a perception on the part of many members of the public that the data was lost to the VA, but it was never lost. These are copies of the data that were lost. And I also want to highlight the fact, to you, the members of this oversight Committee, that while we have been addressing this issue, as you would imagine, double time, we also have been attending to the business of the VA, which is our core mission, which is caring for the health needs and the benefits of our veterans, and of course the burials.

I would point out to you that we have over a million veterans come to us every week for health care provision, and we are taking darned good care of them. Since this theft occurred, it has come to my attention, I have taken many proactive steps on many fronts, but all of them have been guided by one question, the answer to one question, which is what is going to be the best for the veterans? And this Committee and its various Subcommittees has had at least one hearing a week since this theft became public, mostly focused on the elements of the theft and its aftermath.

Other committees have held hearings on this, and we provided briefings for various members of the Congress and their staffs. So for that reason, much of what I say will be familiar to you, I know. But I would like to organize my presentation into a few basic points, and that is what have we done, what are we doing, what needs to be done, and how will we measure progress on these fronts? And again, our goal is, on behalf of the veterans, to make the VA into a first-rate organization in the realm of cyber and information security, just as we have done as an integrated healthcare provider.

Following the theft of this data at the employee's home, we determined or attempted to determine the scope of the loss, and we retained forensic experts. And once the magnitude of this was more fully understood, we began working nonstop to see what steps are appropriate now going forward to protect our veterans.

I directed a series of personnel changes in the office of policy and planning where the breach occurred, the two senior people in that department, as well as the person who had custodial responsibly for this data. I retained an outside independent adviser to me, Rick Romley, the former prosecutor and district attorney in Arizona. I have expedited cyber security awareness training and privacy training for all

VA employees, directed that VA facilities across the country observe Security Awareness Week this week, and it is focusing on assuring that security is an integral part of our workplace culture ethic.

The VA's initial response to this loss was to create a call center with a capacity to handle 260,000 calls, and we reprogrammed $25 million to do that. To date, we have spent $9.3 million in that call center. We have had a total of 212,000 calls. Another thing that we did is a mailing to all of the 17.5 million people for whom we had addresses by matching our data with the IRS to come up with those addresses. The mailing cost was $7 million.

As you well know, we also requested and got the requisite policy approval to seek from you the ability to provide security monitoring for the affected veterans, servicemembers, and family members, and I have quite a bit on that and I think I will demur on that, pending what questions that you might have on that. You know, we hope and pray that is academic, but we don't know that as I sit here.

Let me talk about some specific actions that are going to—that are and will occur at the VA, and again, one of the redemptive parts of this I think is the absolute wake-up call lightning rod to make changes in this organization, some of which I hope will become models for other agencies that I know have some similar complacency and laxity that we have had on information security.

I directed that every laptop computer in the VA undergo a security review to ensure that all security and virus software is current, including the immediate removal of any unauthorized information or software, and application of appropriate encryption programs. But because of the pending lawsuits, this directive has been placed on hold until we obtain further guidance from the courts.

In addition, we have been in discussions with corporations which provide unique data breach analysis to see if the data has been exploited. And we anticipate that we will enter into a contract for that service shortly, and I would add here parenthetically that I think that we should do that anyway regardless of what the outcome of what we are now hoping for, based on today's news. This is not extremely expensive. It is a new technology, but they can tell you whether a body of data is being used, exploited by people who do this, who steal identity and exploit it.

We are making an effort to be responsive to the concerns of you, Mr. Chairman, and this Committee, by directing us to provide detection, protection, and insurance. And that I would say is there, it is pending further information. I directed that the VA conduct an inventory of all positions requiring access to sensitive VA data, to ensure that only those employees who need such access to do their jobs have it. And that they have the appropriate background checks.

And if you could think of a model for this, it is one that you are all familiar with, which is having a security clearance for having access

to classified information, and having a need to know the information. This unfortunately has just not been the standard in our organization. And as you heard me say before, the person who had custody of this data had not had a background check in 32 years, as an example.

We have been in an effort to conduct this inventory of these positions, and then we are working on a program for getting these background checks in place, which is no small task, given the time delays there are on those, and it is costly. We are doing a major IT reorganization within the VA, and it is true, as the Chairman and Ranking Member have said, that the VA has been very highly decentralized, and this is a huge organization that is spread all over the world really from Togus, Maine, to Manila in the Philippines.

And some of that decentralization has been good. It has kept the IT closer to the ultimate user, and I would say that it has also been very valuable and important in the development of the highly vaunted electronic medical records that we have, that lead—I was at a world forum of the American Enterprise Institute recently, where they were universally praising the VA for what it has been able to accomplish in this front.

But it has also, this decentralization, has led to a system that is very, very complex, frequently incompatible, and very difficult to manage. And that has become clear to me shortly after I came into this job 16 months ago. So after reviewing the recommendations of the consultant who had been studying the IT situation at the VA after the ill- fated Core FLS endeavor in Florida in October of 2005, or that is when I made the decision and signed the memorandum directing the reorganization of the IT within the VA. That was last October.

And pursuant to that, now more than 4600 IT professionals engaged in operation and maintenance of the department's IT infrastructure, plus 560 unencumbered positions, have been detailed to the Office of Information and Technology under the direction of the Chief Information Officer. As of the beginning of the new fiscal year coming up on October 1st, those who have been detailed will become permanently assigned there, establishing thereby a new career field within OIT.

Given collective bargaining agreements—

THE CHAIRMAN. Excuse me, Mr. Secretary, if you could hold your spot, okay? Put a little note there in your statement, hold that spot. I have been informed we have three votes. We have a 15-minute vote on the Poe amendment, a two-minute vote on Hefley, and a final passage. So we are going to stand in recess for approximately 25 minutes.

And Mr. Secretary, given your announcement, I am sure that you are going to be asked questions from the press. You have the permission of the Committee to speak with the press and conduct an inter-

view in this room. The Committee stands in recess.

[Recess.]

THE CHAIRMAN. The House Veterans Affairs' Committee full Committee will come back to order.

Mr. Secretary, there is much abuzz about your announcement this morning. We just returned from our votes. Members are feeling pretty good about the news, but don't know whether they can take the next breath until we have learned whether or not anything has been compromised. Sir, when we left off you were still in your opening statement and we want to give you latitude. You are now recognized, sir.

SECRETARY NICHOLSON. Thank you, Mr. Chairman, I am glad that there is some positive buzz for a change, and let me, if I may read an e-mail that I have gotten with an update, which is as follows:

"An FBI spokesman said the laptop computer was recovered in the area, but could not provide more specific information. Forensic tests showed," quote, "the sensitive files were not accessed, according to the special agent in charge, Bill Chase."

So it is still positive, very positive, and we remain hopeful. With that, Mr. Chairman, I would like, if I could, to pick up where I left off, which is I think talking about a very important thing that we have launched at the VA, which I think is pleasing to you and the members of this Committee, which is the major movement of centralization that we are undertaking.

And I had mentioned that we had moved 4,610 people, professionals, engaged in the department's IT infrastructure, under the direct control of the Chief of Information. Plus another 560 positions have been detailed there. And come October 1st or the end of the current fiscal year, these details there will become permanent, and a new career field will be established in the VA, now, for career professionals in IT. That has not ever been the case. And I think that that is a very important, progressive, and needed step.

There are collective-bargaining agreements with our unions that come into play and they have filed grievances in an attempt to prevent this change. And some of this is I think normal. There is a fair amount of anxiety because we are moving people now internally in the organization into a new organization. We hope that we can resolve those things with the union and see and convince them that these people are really going to be better off, because they are no longer going to be hitchhiking career-wise to a different career field than their own specialty.

And in this reorganization all IT professionals are then going to be consolidated in the Office of Information and Technology. And then there is one exception, and I know this is a very important exception to the Chairman, and that is the software developers who reside mostly with VHA and VBA. But even for these, the CIO will be

responsible for their enterprise architecture, their project planning approvals, through the OMB 300 process, funding, and cyber and information security, which we are meeting here today.

So in this concept, I think this is a very big step. I can tell you it is a very big thing inside our organization. And I think a very positive thing. And it is incremental, in my mind, and my goal is for these developers to also be brought under the total control of the CIO. These are the real creative types that are out there, you know, creating these software application programs for medical research, and so on.

Various other functions are being centralized within the VA IT as well. The position of Chief Financial Officer, with budget authority, has been established in the Office of Information Technology. Security has also been consolidated within the Office of Cyber and Information Security in the OIT.

Additionally, I want to assure you that I have been paying close attention to all of these hearings and I have heard your concerns about whether or not the CIO has sufficient enforcement authority to ensure compliance with the deficiencies noted in the past, and to ensure future compliance. I have looked into this a great deal and I agree with you that there has been an ambiguity, to put it mildly, probably, in our directives.

Therefore, as has been mentioned, I have issued a memorandum making it absolutely clear that all responsibilities with appropriate authority, to include enforcement, lie with the Chief Information Officer, and I will say that your interest in this, in this Committee, and you, Mr. Chairman has been very helpful. This is long overdue.

Further I have directed that responsibility for information security be included among the critical elements of all senior executives' performance plans, tying security performance and plans, and the reviews of that, to the effects on the bonuses of those individuals. We have already had several major experts engaged to help us develop a consolidated data security program. These include many recognized names in the industry. They will be supporting a program whereby responsibility, authority, accountability, and enforcement are consolidated under the CIO. We have engaged one of the world's leaders in the expert field of cyber and information security, which is a Carnegie Mellon SEI, to independently verify and validate our security plan and measure our implementation.

In addition, we will be retaining an acknowledged expert on program management operations to manage this entire process of transformation. I am also pleased to announce that just yesterday we entered into a contract with IBM to assist us in implementing our overall IT realignment plan. IBM is a recognized expert in IT integration. They themselves have experienced the difficulties of IT realignment, but I am confident that with our commitment and their assistance, we will meet our goal of completely transitioning to a fully

realigned IT management system.

The range of IT programs administered by the Department of Veterans Affairs on behalf of our veterans is extensive. Many of these programs or services require that the IT to back them up be interactive, with VA professionals having a need to access and manipulate data elements in the course of providing health care or benefits, often in locations outside of the VA facility. For example, VA employees checking on the care that a fiduciary is being provided with respect to an incompetent veteran, loan guarantee employees doing field examinations of appraisers, or home health care providers for housebound veterans, and I could go on and on. As a result, the array of hardware and software, where it is located, the number of systems, the number of persons having access to it, how that access is granted or denied, how the data is utilized, and by whom, what background checks are needed; all have grown tremendously over the years.

These are areas, then, that require our immediate review and, where necessary, remediation. This VA data theft has been a real wake-up call to us. IG reports in past years have highlighted specific weaknesses. But as an institution, the VA did not respond to those with a sense of urgency that in retrospect clearly was called for. With the benefit of hindsight, that need for urgency is overwhelmingly apparent to me today. We recognize that we must change the culture of this department, and we have embarked on doing that.

On May 24th I instructed the deputy secretary to establish a three-phase program to assess existing conditions, strengthen internal controls, and establish enforcement mechanisms. The assessment phase is now almost complete. We are now reissuing guidelines and regulations clarifying and emphasizing requirements, and the ramifications for failure to follow them.

In addition, I have directed that all VA's sensitive data be kept on VA equipment, such as laptop computers. In the past many employees have utilized their own personal computers to conduct VA business. We are assessing just who is doing that and why, and we will be issuing guidance regarding that in the near future. I have also directed that previously authorized work procedures, which allowed VBA employees to transport hard copies of claim folders to alternative work sites be stopped. It is a government-wide practice to encourage telework or telecommuting, especially here in the Washington area. Yet we must assure that our policies and procedures implementing this are such that sensitive data relating to our veterans is properly protected. I have asked our Acting Under Secretary for Benefits to review and revise his own guidance to his staff in this area to ensure the protection of the veterans' vital records and sensitive data prior to resuming this practice, if at all.

As I mentioned, the VA is revising its regulations, policies, guidelines, and directives, in the entire area of information technology and

security. We are working to assure that we have clear guidance for all VA employees in place and that they are fully trained in what is required of them, and that compliance is monitored.

We are revising VA directive 6500, which sets forth the guidelines for information security and the enforcement mechanisms pertaining to that. This is on a fast track, and I anticipate issuing that directive very shortly. But I am convinced that coming out of a very bad situation, we can make the VA a model for data security.

How are we going to measure our success in this endeavor? Well, I am putting forth a slate of directives enhancing the authority of the CIO, creating accountability throughout the system and requiring measurement, and I have mentioned the consultants that we are engaging to help us with that. Performance metrics will be tracked by my office in conjunction with the CIO until we become that model to be emulated by others. And of course, we have our own Inspector General, who has pointed out shortcomings in the past. And while the IG is housed at the VA he is independent, reporting directly to the President. I think you will see that he offers a critical overview of what we are doing. And initially that will be to correct deficiencies noted by him in the past.

In addition, we are scored each year on FISMA compliance. And as I have noted in the past, we have received abysmal scores. That is unacceptable and we must and we will do better. In the area of legislation, Mr. Chairman, the Health Insurance Portability and Accountability Act, known by you all I am sure as HIPAA, governs all aspects of the privacy of sensitive information related to a person's health. HIPAA provides for criminal penalties of up to 10 years' imprisonment and a fine of up to $250,000 for its intentional misuse.

There is no comparable law pertaining to the misuse of other non-health sensitive personal information. And I believe that Congress should enact such a law. Someone intent on fraudulently using personal information may think twice if he or she focuses on severe penalties that could be encountered for such a crime. I also now serve on the President's new task force on identity theft and I will be making similar requests there for tougher laws, greater deterrents, and other actions that will minimize the likelihood of an event such as this occurring again.

In conclusion, Mr. Chairman, unfortunately a terrible thing happened, monumentally terrible. It has outraged me and so has the slow response by some of my very good subordinates, but I am the responsible person, and it is to me that I think you are entitled to look to see that our victims are treated right and that this place gets fixed. And it will not be easy, and it will not be overnight, I am convinced that we can do this. And we are already on the way I think to establishing a new culture of security within the VA with the policies and procedures and the people in place to maintain them.

That concludes my testimony, Mr. Chairman, I would be pleased to answer questions.

THE CHAIRMAN. Thank you very much, Mr. Secretary.

Under Secretary Tuerk, Under Secretary Perlin, Deputy Secretary Mansfield, Assistant Secretary Aument; the four of you have written testimonies, do you not?

All answer in affirmative. Would you submit that statement for the record?

[All answer in the affirmative.]

The Chairman. Hearing no objection it is entered, so ordered.

[The statements of Mr. Tuerk, Dr. Perlin, Mr. Mansfield, and Mr. Aument appear on p. 58, p. 67, p.76, and p. 84, respectively.]

THE CHAIRMAN. Other witnesses are here to accompany the Secretary, and if members have questions of them we have a roving microphone. If these witnesses will please rise when recognized.

The Honorable Tim McClain, General Counsel to the Department of Veterans Affairs. You may be seated. Mr. Tom Bowman, who is the Chief of Staff to the Department of Veterans Affairs. Mr. Dennis Duffy, the Acting Assistant Secretary for Policy, Planning, and Preparedness, for the Department of Veterans Affairs. Missing? Sorry, please stand. If you did, I didn't see you. I apologize. And Mr. Mark Whitney, with Policy, Planning, and Preparedness, for the Department of Veterans Affairs. Thank you.

Mr. Secretary, in your opening statement you referred to a memorandum. I would ask unanimous consent that your memorandum signed and dated June 28, 2006, entitled, "Memorandum for the Assistant Secretary for Information and Technology," subject line, "Delegation of Authority for the Responsibility for the Department Information Security," be entered into the record. Hearing no objection so ordered.

[The memorandum appears on p. 98]

THE CHAIRMAN. I would also like to publicly thank Health Net. Health Net is a company that does business with the VA, that they supplied $25,000 and matched the reward money. And I think they should be publicly recognized for what they have done.

I will also ask Mr. Secretary, and I do want all the members to have their opportunity to talk with you, but I do want you to share with us these two other breaches that have occurred: the one in Minneapolis, whereby you had an employee put a laptop computer in the trunk of a car and the car was stolen and information was compromised, and you did have two cases of identity theft. The other, I would like to discuss the circumstances, and I would like to know about the notification procedures regarding the loss of a backup tape at the regional counsel's office, whereby they are missing 16,538 legal cases in the

city of Indianapolis. Mr. Secretary?

SECRETARY NICHOLSON. Yes, sir, Mr. Chairman. The incident in Minnesota was brought to our attention by a postal inspector, who had reason to believe that two people, two patients in one of our extended care facilities, was possibly having their identity exploited, and that led to a fact-finding endeavor that the IG has been investigating this. And it turns out that the VA had a financial auditor in that facility to audit the income status of certain patients, because there is a means test that goes on for some of them in those facilities. And that person put some of these patient files in the trunk of a car, of a rented car, and that car was stolen. And there were I think 60- some, 66, I believe, people's information was in that, they were paper copies, and that happened in 2005, the car was stolen in 2005.

This did not come to our attention until, as I said, the postal inspector sensed that two people were being defrauded, and so we have the IGs inspecting, conducting an investigation and we are, you know, going back to the responsible person, waiting for the final report of the IG. Another case where the importance of this was not sensed and dealt with by that employee. The Indianapolis—

THE CHAIRMAN. Sir, we have a question on Minneapolis.

SECRETARY NICHOLSON. Yes?

THE CHAIRMAN. When you said 66 people, are these 66 veterans?

SECRETARY NICHOLSON. Yeah, I think they—

THE CHAIRMAN. All right.

SECRETARY NICHOLSON. I am told yes. I pause because there are a few people in—facilities who are not—

THE CHAIRMAN. And an audit of materials, would it indicate that it also contained necessary granulated information such as name, address, Social Security numbers?

SECRETARY NICHOLSON. Yes, sir.

THE CHAIRMAN. And with regard to the notification of all 66 veterans, have they been notified with regard to the loss of this data?

SECRETARY NICHOLSON. They have been notified, yes, sir.

THE CHAIRMAN. And are you considering taking the same action with regard to these 66 veterans as you were going to take with regard to this stolen laptop and hard drive, with regard to credit monitoring?

SECRETARY NICHOLSON. Yes, sir, credit monitoring.

THE CHAIRMAN. And insurance?

SECRETARY NICHOLSON. Yes.

THE CHAIRMAN. Okay. All right, let's talk about Indianapolis.

SECRETARY NICHOLSON. All right. Indianapolis is more recent, where there is a backup tape that is missing. This occurred, I think, on May 5. It was in the regional counsel's office in Indianapolis, and the general counsel was notified of this on May 23rd. It involves 16,500 individual cases. And again, the IG is investigating this, and we await

their report for you know, the actions that we will take with respect to personnel. We are notifying these people, and we plan to give them credit protection as well. The General Counsel is here, Tim McClain, if he cares to add anything to this, I would welcome him to do that.

There, the reporting was better than it has been. But the practice, I mean, it happened, and we have a tape missing. The data again is not missing, in that there is a daily chronology of these cases, a lot of this is litigation and stuff that they are tracking electronically, and so they have the day before and the day after, so that the data is not missing to us, but that tape is missing, with those individuals on it.

THE CHAIRMAN. Well, may I ask your counsel. Mr. McClain, if there is a remote mike. Mr. McClain, if there are 16,538 legal case records, would it not be true then that these files would have contained once again granulated information regarding the veteran, perhaps their dependents, some could be VA employees, Social Security numbers, claim numbers, addresses, date of birth, legal case numbers? Would that be an accurate assessment?

MR. MCCLAIN. In some cases, yes, Mr. Chairman.

THE CHAIRMAN. And in these case files, then, could there also possibly be embedded case-related documents such as claims, court documents, patient medical records, property descriptions, other personal information?

MR. MCCLAIN. Yes.

THE CHAIRMAN. With regard to the backup procedures that occurred prior to the loss, could you explain what occurred in the regional office in Indianapolis, with regard to how a backup was conducted and how these tapes were safeguarded?

MR. MCCLAIN. From what I have learned about this particular office, and how it was run, there is a computer room that the computers and the servers that run this particular system. This is a homegrown software system known as GC Laws. It is something that we developed and had implemented in 2002, and it has been in development since then. It is a case tracking and attorney time tracking software.

Cases can be anything from a 30-minute telephone call with someone such as the VISN director or the medical center director, to a full-blown Federal Tort Claim Act case or medical case. And so, we define a case essentially as you are giving legal advice in a substantive area and you are doing it for about 30 minutes or more. That is why the number of cases are not going to be the same as the number of actual individual identifiers in the GC Laws area. Every day, this system, which has information only from this particular region—we have 22 regions that this is region 22—and they then back up this server that the GC Laws software resides.

THE CHAIRMAN. Do you know the territory of that region?

MR. MCCLAIN. Sir, it is the regional counsel offices in the Federal

building in Indianapolis, which I know you are very familiar with, sir.

THE CHAIRMAN. That would include parts of Ohio, Michigan, Illinois, Kentucky—

MR. MCCLAIN. It would include all of Indiana and Kentucky.

THE CHAIRMAN. Please continue.

MR. MCCLAIN. This particular office maintained two weeks' worth of backup tapes; first Monday through Friday, second Monday through Friday. Every night, the tape would be changed, and then put into its appropriate—the one taken out would be put into its appropriate slot. On May 5th, it was discovered by the information security officer that the tape for the second Monday was missing.

THE CHAIRMAN. Are you aware or not whether it was a common practice for a backup tape to be taken home with one of your lawyers?

MR. MCCLAIN. I am not aware of that, sir. The backup tapes for the most part stayed in the room.

THE CHAIRMAN. I would invite you to explore. Did the tape contain confidential and privileged information?

MR. MCCLAIN. There most likely was privileged information that would have been generated in Federal tort claims cases, which would have been attorney-client privilege.

THE CHAIRMAN. The room where these backup tapes are stored, is it secured or unsecured?

MR. MCCLAIN. It has a lock on it, but that is all. It is in the office and it has it on the door.

THE CHAIRMAN. I want to thank you, Mr. Secretary. Mr. Filner had asked for a timeline yesterday and we have received the timelines with regard to individuals for the case in Maryland. Mr. McClain, have you put together a timeline with regard to notifications, with regard to this case in Indianapolis?

MR. MCCLAIN. Yes, sir, we have a general timeline.

THE CHAIRMAN. Okay. Just for curiosity's sake, why didn't you tell us about this yesterday?

MR. MCCLAIN. That was my oversight, sir. I owed you that. I was concentrated on this particular situation that we have. And there is no question you should have been notified.

THE CHAIRMAN. Mr. Secretary—let me ask Mr. McClain. When were you notified with regard to the loss of this tape?

MR. MCCLAIN. May 23rd.

THE CHAIRMAN. Missing on May 5th, you were notified on the 23rd? Mr. Secretary, when were you notified with regard to this lost tape in Indianapolis?

SECRETARY NICHOLSON. I think that I was notified either that day or the next day, Mr. Chairman.

THE CHAIRMAN. The 23rd or the 24th?

SECRETARY NICHOLSON. Yes, sir.

THE CHAIRMAN. This case runs parallel to what was occurring in Maryland, with regard to the notifications, and procedures. We are going to need to learn more about Indianapolis, Mr. Secretary, and I am pleased about your opening statement, because you exercised leadership here over the last four weeks. But there is definitely more that we need to learn about this case in Indianapolis. Because this is a tremendous exposure potential with regard to your legal system, Mr. McClain.

MR. MCCLAIN. Yes, sir.

THE CHAIRMAN. The last thing I would ask, with regard to the memo that has now been submitted for the record dated June 28th, Mr. McClain, as General Counsel for the VA, do you believe that this memo complies with FISMA?

MR. MCCLAIN. Yes, sir, I do.

THE CHAIRMAN. Congratulations. I yield to Mr. Filner.

MR. FILNER. Thank you, Mr. Chairman. And Mr. Secretary and your staff, we are all feeling better this morning. You said, the saints were smiling on you. I guess that was for your service in the Vatican, not on the RNC.

SECRETARY NICHOLSON. St. Anthony.

MR. FILNER. And we are all fortunate of course, we don't have to spend the money apparently for credit monitoring. I was upset about the proposal for those dollars from an administration that spends hundreds of billions in a supplemental in the war on Iraq, yet wouldn't do a supplemental for the veterans, of $130 million. It was going to take money out of food stamp programs or student loans, so I am glad that we won't have to argue about that one. Let's hope that we don't.

And like the Chairman, I thought your statement was very good and powerful. I wrote down some quotes I thought were very welcome here, the recognition of real deficiencies, a sense of urgency, the "wake up call." I think those are all powerful statements, and I hope that they echo through the VA system.

There is a famous quote that says "Those who cannot remember the past are condemned to repeat it." I know you all want to look forward and clear up some of the mistakes and errors and deal with them. I still think there is a sense of denial, Mr. Secretary. Mr. McClain just referred to this whole thing, as "the situation." Yesterday he called it an "incident." You called it a "wake-up call." I call it a major disaster. And I think people have to accept that we may have come out lucky on it, but it was a true disaster. Until people get that, I don't think we are going to get the change throughout the system that you need.

The timelines that we have looked at have showed some real programmatical errors, I think. And I hope you deal with them. We are grateful that the FBI was able to do something, but from the

timelines it looks like it took almost a month before they were even brought into it. It maybe would have gone faster, it looked like to me after the initial police report there was all kinds of internal stuff and then you were notified and you called the White House. And then the FBI, and so it took some time for them to even be involved in it. And I find that is a little disturbing, if that is the case.

All right, I would just like to take a few minutes, if I may, Mr. Secretary—but your statement on the "F" grades from FISMA about "determined to change those" is again, I think that needs to echo through the whole system, and I appreciate those statements.

With regard to the personnel and the errors that were made in the last eight weeks, has anybody been given a notice that they are going to be fired in this whole process?

SECRETARY NICHOLSON. Yes, sir. One person has been fired, because—he could be fired summarily because he was a political appointee, who was the Deputy Assistant Secretary for Planning and Policy. The Acting Assistant Secretary is a career employee and has rights and due process. And so through a mutual arrangement, he retired, because he is eligible for retirement. Those are the two senior guys, those are the number one and the number two guy in that department.

The person who had custody of the data that was stolen I will tell you quite frankly, when I heard about it I said, "he needs to be fired, fire him." I was then told "you can't fire him, but you can put him on administrative leave with pay," which we did, we have done. And we have initiated a process to have him terminated from Federal employment.

MR. FILNER. Based on what?

SECRETARY NICHOLSON. Based on the advice that I was given that he did this in violation of existing policies. And that he acted irresponsibly and negligently in having that kind of data, you know, that could be stolen.

MR. FILNER. The reason I am concentrating on this, Mr. Chairman, is I think there was an initial sense, what you called the Abu Ghraib mentality, to blame it on the lowest person possible. I would like to enter into the record several documents that have been redacted from names, so I think it is perfectly acceptable, what is called an "employee home use amendment" to the VA's license agreement for the software, that this employee was authorized to have that data at home. Also, there is a property pass that was issued to him that he was authorized to have the laptop at home. And a third document, again redacted from the names, that he had authority for access to the files.

THE CHAIRMAN. Does the gentleman ask unanimous consent that these be made part of the record?

MR. FILNER. I do, sir.

THE CHAIRMAN. Preserving the right to object upon further examination—

MR. FILNER. Sure. Under the advice of counsel, they have been redacted of any personnel specifics.

THE CHAIRMAN. I have no objection to entering these in the record. Any objections? So ordered, they will be made part of the record.

[The information referred to by Mr. Filner appears on p. 101]

THE CHAIRMAN. Mr. Secretary, are you familiar with these documents?

Secretary Nicholson. No, I am not. I would like to take a look at those if I could. I have heard about those, but I don't think I have—

MR. FILNER. You have heard of them, did you say?

SECRETARY NICHOLSON. I heard that they existed, yes, sir.

MR. MILLER. Mr. Chairman, can we get copies?

THE CHAIRMAN. Yes.

MR. MILLER. They are all being passed out over here?

THE CHAIRMAN. I am not sure.

MR. FILNER. We will get copies to you.

THE CHAIRMAN. Let us allow the Secretary to look at the three documents and—Ma'am, are you passing out the three documents? All right.

MR. MILLER. And the minority members have them as well.

THE CHAIRMAN. Yes.

SECRETARY NICHOLSON. Okay, all right.

THE CHAIRMAN. Mr. Secretary, you are familiar with these three documents?

SECRETARY NICHOLSON. I am looking at this document, first time I have ever seen it.

THE CHAIRMAN. Mr. McClain, are you familiar with these documents?

MR. MCCLAIN. Yes, sir, generally.

THE CHAIRMAN. Generally. Mr. Duffy, are you familiar with these three documents?

MR. DUFFY. Again, generally, yes.

THE CHAIRMAN. All right. Mr. Filner, you are—

MR. FILNER. My sense is, and you can comment on this, Mr. McClain, that the employee was authorized to remove these files, and that was the first thing he was going to be removed for. And gross negligence, I mean, he got all the approvals that he was supposed to have, and I am told that even in the—well, I'll ask about this later.

It looks to me that the gross negligence is in the policies. There is no policy. You have said he violated the policy. I don't know of any policy that he violated. That is the real negligence, that there were no policies.

He notified the police 52 minutes after the theft occurred, accord-

ing to the police report. And your staff didn't notify you for 6 to seven days. I don't know which is more gross.

SECRETARY NICHOLSON. Thirteen days.

MR. FILNER. I am sorry, 13 days. Thank you. I think there is more gross negligence from the uppers than this poor guy at the bottom. So what policy did he violate and why is it more negligent to not tell you about what happened and not tell the FBI et cetera, et cetera?

SECRETARY NICHOLSON. Mr. Filner, we have taken these actions and we took them based on the reasons that I have given you. This employee who has, you know, rights—has asserted those rights and he is entitled to a hearing and will have that hearing, and that is pending. And with all due respect, Sir, I think it would be wise for me not to comment further on the disposition of this employee.

MR. FILNER. I understand that, Mr. Secretary. I introduced them, again redacted for names, to show that we didn't want to have one person at the very bottom of the food chain held responsible for the biggest data loss in Federal Government history. I mean, that is what it is, and we are saved by something or other but it is still there. It is still happening. And I guess I would like to ask you, and you don't have to answer now, but the powerful statement you made in terms of changing the culture, which is still going to be a hard job, but I think you are. I think the Chairman and I would agree that you are doing exactly what has to be done, that you have to hold folks accountable for the "F" grades, the previous FISMA things, for the delay in reporting, for all that was going on. I appreciate the one mistake of a good employee is not the only thing in this record, but I think you have to make a bolder statement about accountability, with some personnel changes, is my sense. You don't have to comment now, but I think our sense of you as trying to change the culture would be enhanced by that.

I may say one more thing for the record, the Secretary took the initiative just a little while ago, pulling me aside and saying, "let's get on a more personal note here." I appreciate that very much. I think we are both trying to do the best we can for veterans. I'll try to do better in terms of personal actions, but I appreciate your taking the initiative, and as always, Mr. Chairman, we are saved by our spouses who are working together for the PVA annual gala dinner.

Mr. Secretary, we want to do the best for veterans. We want to help you do that job. You have taken the first step, and we do appreciate the announcement today.

Thank you Mr. Chairman.

THE CHAIRMAN. Mr. Filner, I do not question the spirit of your personal enterprise. I appreciate the bipartisan fashion here over the last four or five weeks that we have worked together, all of us on this Committee have worked in a bipartisan fashion. This really goes back with Art Wu and Len Sistek, almost seven years and I think

that investment of time is paying off dividends.

And Mr. Secretary, I am going to yield to Mr. Brown, but you know, I enjoin and affiliate myself with the comments of Mr. Filner. The statement that you give us today compared to the statement that you gave us several weeks ago, you cannot compare the two statements. You came in here today as a man in charge. You told us in response to a moment of your leadership that you were going to do that, that you were going to exercise leadership and take control of this, give assurances to veterans, and make changes to the system. And you have come in here with your bold strokes and bold initiatives and for that you are entitled to be recognized.

Mr. Brown, you are recognized.

MR. BROWN OF SOUTH CAROLINA. Thank you, Mr. Chairman. Mr. Secretary, a recent IG report identified vulnerabilities relating to offshore subcontractors who have access to VA medical transcription data. I know that you were confronted with this question by Chairman Walsh earlier this week. But this Committee is also very interested in your views on the role of offshore contractors and subcontractors and their access to sensitive health-specific data on US veterans. Would it be prudent in your opinion to consider contracting limitations for offshore entities in order to mitigate the risk of data loss or theft?

SECRETARY NICHOLSON. Thank you for that question, Mr. Brown. The case you are referring to is one that I have looked into. It was a case where we had entered into a contract, the contractor subbed, and he subbed to another sub, doing back-office work in India. The Intermediary sub went bankrupt. Our contractor had paid the first sub that went bankrupt, and the working folks in India weren't paid. I go into this detail to illustrate the vulnerabilities of this.

So they weren't paid, they came to us. And they have over 30,000 entries of sensitive data of veterans that they were working with and they said that "You either pay us or we are going to put this online," which to me is a microcosm of the vulnerability that we have in this whole field, where we give people access to this data that we don't know enough about. Even our own employees, let alone people offshore.

So the answer to your question is clearly yes. We should endeavor not to have these contracts end up offshore for that reason, particularly.

MR. BROWN OF SOUTH CAROLINA. How many other contractors are you dealing with, Mr. Secretary, besides this one? Do you know?

SECRETARY NICHOLSON. One minute. The only one that I know of right now, we are looking at this, but there is one other right now and that is a contract that we entered into with a company to provide the general management of the homes that we repossess under our VA guaranteed loan program. We have a master contractor to

go through the foreclosure, take possession, refurbish, and remarket those homes. They do their back-office accounting work, have it done offshore. That is the only one that I know of right now. By the way, we are reviewing that contract, because it is coming up for renewal and that is a relevant item in that discussion that we are having.

MR. BROWN OF SOUTH CAROLINA. So I guess your opinion, and you are going to try to lessen any further exposure by going offshore with some of the information gathering?

SECRETARY NICHOLSON. You know it is this globalized digital world that we are living but I think it just creates too many vulnerabilities for us.

MR. BROWN OF SOUTH CAROLINA. Thank you. Thank you for your service, Mr. Secretary.

THE CHAIRMAN. Mr. Brown, I want to yield—but may I ask a follow-up? It provides too many vulnerabilities to us? Following Chairman Brown's questioning, this issue about subcontracting and offshoring, outsourcing, these present grave concerns to you? They do?

SECRETARY NICHOLSON. Yes they do.

THE CHAIRMAN. Okay. All right, do we have any of our call centers that are subcontracting coming of places such as China? Are you aware?

SECRETARY NICHOLSON. No, sir. No, none that I am aware of.

THE CHAIRMAN. Is it possible that service centers for your medical devices might originate from China? Is Mr. Howard in the room?

SECRETARY NICHOLSON. I might best refer to Dr. Perlin for a detailed answer.

DR. PERLIN. Mr. Chairman, with respect to medical devices, many of the major manufacturers are not American: Siemens, Fujitsu, Motorola, Philips, et cetera, if you want any MRI or CAT scan or angiography suite or radiology. I personally am not aware if any originate from China but I would not be surprised if some devices are manufactured there.

I would note that the servicing of the device is electronic in 2006. And there is interaction with that. I would have to defer to Mr. Howard for any further elaboration.

THE CHAIRMAN. Mr. Howard?

GENERAL HOWARD. Sir, I really can't add any more to that.

THE CHAIRMAN. All right. Well, I think if you take a look, you are going to find out perhaps that it may be true that one of the service centers for one of your medical devices comes from China. As the world gets smaller, the more we are interconnected, and then as we seek to try to protect our veterans I think we are going to find we have some serious problems.

Ms. Brown?

MS. BROWN OF FLORIDA. Thank you, Mr. Chairman, and thank you for holding this hearing. Yesterday, I had the pleasure of meeting

with the Veterans Widows International Network. I am looking forward to working with them, but as we move forward for the Independence holiday, we cannot forget why we are here, and we are here all of us to serve the veterans.

And Mr. Secretary, in your testimony you stated that you have just issued a memorandum that all functions lie within the CIO. Which guarantees will you make that the lawyers will not get involved and rule the exact opposite like what happened to your predecessor?

SECRETARY NICHOLSON. If I understand your question correctly, Madame Congresswoman, my answer is yes, that is the purpose, is to centralize this, and to have residing with the same person, and not just responsibility but the authority.

MS. BROWN OF FLORIDA. Yes sir, I understand what you are saying. But what I am saying is that your predecessor did the exact same thing: issued the memorandum saying that that person had the responsibility, but the lawyers ruled just the opposite.

SECRETARY NICHOLSON. I am with you now, and that has changed. We have changed that. We moved these people to come under the CIO. A lot of objection, debate, just we have done it. And they now are under that Chief Information Officer.

THE CHAIRMAN. Mr. McClain, could you help and be responsive to the gentle lady's question?

MR. MCCLAIN. If I understand the question correctly, is that the Secretary ordered a directive and then my office, as Office of General Counsel, would say that it was invalid or ruled differently?

MS. BROWN OF FLORIDA. Yes, just the exact opposite.

MR. MCCLAIN. Mr. Chairman, I would basically rely on my testimony from last week, where this was gone into in depth as to exactly what that opinion was. And both opinions from 2003 and 2004, essentially, was in a nutshell an interpretation of FISMA and what could be delegated. And this delegation memo that we have here today is actually what was delegated under FISMA.

MS. BROWN OF FLORIDA. I have a follow-up question for you.

MR. MCCLAIN. Yes, ma'am?

MS. BROWN OF FLORIDA. In reading the information, what was passed out as far as the employee that took the information home and had clearance to do that, a memorandum, and also directly afterwards, reported that it was stolen, I mean, just right away, but this is a person that is going to be fired, can you clear that up for me? Because I can see that we are headed to a lawsuit with this, because he had permission, and he had it in writing, a memorandum.

MR. MCCLAIN. First, I am not going to comment directly on pending personnel action for this employee, because it is still pending. There has been no final decision made in this employee's particular case. But the documents that were presented by Mr. Filner, one being a justification for access to Social Security numbers, that would be part

of his job to look at those. Another one is an employee license to have software at home, and the other one is a laptop property pass that does not relate to this laptop.

Ms. Brown of Florida. That's your answer?

Mr. McClain. Yes.

Ms. Brown of Florida. Well I guess, you know, I am not a computer geek, but it would be no point in using the software at home if you know, you couldn't use it.

Mr. McClain. Yes, ma'am, I understand that once again I would like to say that the process is continuing, and for the integrity of indeed this due process that the employee is entitled to, I can't directly comment on the pending personnel action.

THE CHAIRMAN. May I?

MS. BROWN OF FLORIDA. Yes, sir.

THE CHAIRMAN. We are in a touchy area. My colleagues, What I feel a little uncomfortable with is that we interviewed this individual. The Counsel for Minority and Majority, along with the staff directors of oversight, interviewed the individual. And these were some of the documents, and I am a little uncomfortable for us to move this into the public arena, because this individual has rights.

MS. BROWN OF FLORIDA. Yes.

THE CHAIRMAN. Ms. Brown—

MR. FILNER. If I may—

THE CHAIRMAN. Yes.

MR. FILNER. Ms. Brown, the particular property pass Counsel referred to was just one of a series of authorizations that the employee had. I don't know if the number of this one matches, but there were a series. Certainly he believes for several years that he had the authorization to take it home.

MS. BROWN OF FLORIDA. Just a follow-up question then, with the Secretary. Mr. Secretary, I know that everybody is breathing a sigh of relief, but I want to know whether or not we are going to continue to monitor the situation to see whether or not the integrity of the information that was out there, are we still going to give the veterans the assurances that we are going to monitor the credit reports? I mean, where are you with this?

SECRETARY NICHOLSON. Well, I think that is a very fair question. You know, it is dynamic. Things are happening even since we have been in this room. But my feeling about it right now is that we should engage the unique capability that we have to see if data are being exploited. That is not relatively expensive to do that, and we could do that, and then I think we ought to keep an eye on, to make darn sure that this data has not been exploited, or has not, you know, been copied, which would be subject to being exploited. And I think we need to remain vigilant.

MS. BROWN OF FLORIDA. All right. Thank you, Mr. Chairman, Mr.

Secretary, I yield back the balance of my time.

THE CHAIRMAN. Thank you, Ms. Brown. My colleagues, the Secretary is accompanied by the Deputy Secretary. Two of the Under secretaries could not be here. So we have his Assistant Secretary. Sir, what should I say? You haven't been confirmed by the Senate, and that is why you are not at the witness table.

The reason we have them all here is for you to be able to ask questions. As we learned from the Under Secretary, the CIO did not have certain authorities to enforce. Therefore the enforcement of all these directives and rules really lay with these gentlemen.

Chairman Miller, you are recognized.

MR. MILLER. Thank you, Mr. Chairman. Mr. Secretary, is somebody from the Board of Veterans Appeals involved in looking at the security issues? And the reason I raise the question is that many of us recall several years ago that an employee from VBA was found to have many files in boxes in their garage.

SECRETARY NICHOLSON. Yes. Judge Terry has been involved in the many meetings we have had on this. I will say that they do have a program whereby they take files home, the judges. But we have looked at it very carefully, and it has been prescribed, it was authorized, and they are in locked containers en route. They are to be put in locked containers, when they are not being worked on at the residence, and in locked containers coming back. We have made a few spot checks on that, and it looks like there is good compliance on that. So we have not made that change.

You noted in my testimony that with respect to the Veterans Benefits Administration, they were taking files home for adjudication. I have stopped that because it was not tight enough. So we are, they are very engaged with us on this and I think, you know, getting the message as well.

MR. MILLER. Going back to the backup tape, is it assumed missing or potentially stolen?

SECRETARY NICHOLSON. I think that is an open question. I would ask General Counsel, do you have a view?

MR. MCCLAIN. [Inaudible.]

SECRETARY NICHOLSON. We are captioning it as being missing. It is missing, and the IG is investigating it. I don't know.

MR. MILLER. And I asked the question that way because I think if you were framing it that you think that somebody took it, that the chances would be different from the laptop scenario, where it just happened to be that somebody took a laptop that had the data on it, versus somebody knowing that they have now in their possession a backup file and you could—I would assume that something nefarious would be intended with that information. And so I was wanting to know, you know, at what point do you treat it differently from being stolen, to missing?

SECRETARY NICHOLSON. I don't think we treat it very differently. We are notifying all the people involved. We are setting up credit monitoring for them. I don't think with respect to the effect of people that it makes much difference.

MR. MILLER. And back to the records that the Chairman was referring to that were entered into the record, the three documents. Is there anything in these three documents that indicates—not gives the impression or not gives an assumption, but indicates that the employee with these documents had the ability to take home that information? I don't read that, but I am just wanting to know if there is anything in here that I am missing.

THE CHAIRMAN. Does the gentleman mean ability or authority?

MR. MILLER. Either. Obviously, he had the ability.

MR. FILNER. Would you yield for a second, Mr. Miller?

MR. MILLER. No, sir, on my time, and I would like to hear the Secretary.

SECRETARY NICHOLSON. Chairman Miller, I am going to demur. This is a pending personnel action, and I think for the protection of the affected employee and the integrity of the system, that we probably shouldn't discuss this any further than we have. He is going to have a hearing, and a fair hearing.

MR. MILLER. And as he should. You know, it is unfortunate that in this entire incident that you had an employee that had he not come forward and said that he had this information on this laptop, VA may never have known that it was on the laptop. They may have known that the laptop was gone, but not that the information was. And I am glad to hear that he will get the due process that is due. And I yield to my friend Mr. Filner.

MR. FILNER. I just wanted to point out that one of the forms says "home use," authorization for home use. And the other one says a property pass to take home.

MR. MILLER. —reclaim my time. Well, on the license agreement, and this gets outside of that so this is not the employee in particular. An employee that is there today has this signed, the software. Is there anything this software is used for other than—I mean, other data that is in it, could it be used for something else? I am just trying to get to the fact that I think this is a stretch, and I am wanting to know if the software can be used for anything else other than what he was using it for? Other data collection?

SECRETARY NICHOLSON. Well, I will give you, you know, a general answer that yes, I mean, the software has different applications that would make it available for different kinds of use and collations.

MR. MILLER. Thank you, that answers my question.

THE CHAIRMAN. Chairman Miller, would you yield for just a second?

MR. MILLER. Yes, sir.

THE CHAIRMAN. Mr. Secretary, you notice that members have been asking questions about the firing of the employee. I would also note that your testimony, well, actually, while you were waiting to testify on the second panel before the Appropriations Subcommittee, that expert witnesses talked about their concerns about immediate firing of employees, that it could have a chilling effect with regard to future losses of data.

I would note that the case that you discussed here today with regard to Minneapolis was a case whereby you were not notified through internal sources. You testified to us that it came from a postal inspector. So I think what you are finding is members have concerns here in how, as the man in charge, you want people to be able to tell us what the vulnerabilities are, and what has gone wrong; if something is lost, please tell us. If they feel that they will lose their job because of it, we may never know, and the vulnerabilities could hurt our veterans, and I think that is what I am sensing from the questions of Mr. Miller, Ms. Brown, and some others. I just wanted to note that to you, Mr. Secretary. Yes, I yield back to the gentleman.

MR. MILLER. Thank you. One other question, are you aware your cyber security chief is resigning as of today? And if so, do you know why?

SECRETARY NICHOLSON. Am I aware that my cyber security chief is resigning today?

MR. MILLER. Yeah, is there any truth to that?

SECRETARY NICHOLSON. I am not aware of that.

MR. MILLER. Is anybody at the table aware of that?

GENERAL HOWARD. The answer to that is yes, sir. We were notified today.

MR. MILLER. And the Secretary wasn't?

THE CHAIRMAN. You didn't tell the Secretary?

GENERAL HOWARD. I told the Deputy as he came in.

MR. MILLER. No further questions.

GENERAL HOWARD. I got an e-mail about half an hour ago that it was official.

THE CHAIRMAN. Wait a minute. Mr. Miller, you still have the time.

MR. MILLER. I yield to you, Mr. Chairman.

THE CHAIRMAN. Thank you. Your CIO has resigned, your Chief Information Officer resigned not long ago. Now your cyber security man has resigned. Mr. Howard, do we know why the CISO has resigned?

GENERAL HOWARD. Sir, about two weeks ago he gave me a letter of recusal, that he was thinking about leaving. I convinced him to take it back, you know, that we needed his service and all of that. And just the other day, he handed me another one with no date as to when he was going to resign. And as I mentioned, you know, I just got an e-mail a while ago that it is effective. I think the date on my e-mail was

13 July or something like that. As far is I know, it was due to pressure on his family due to what has been going on. You know, he has been working extremely hard. He has been in charge of the forensic work, for example, that has been going on, working very long hours. They are all under a great deal of pressure, you know, to get at the details, produce the facts. And I think most of it was family, but it was probably just the work environment as well.

THE CHAIRMAN. All right, Dr. Snyder, may I ask a question, or Mr. Miller?

Have you informed the Secretary?

GENERAL HOWARD. Sir, I told the Deputy Secretary.

THE CHAIRMAN. Have you informed the Secretary, Deputy?

MR. MANSFIELD. No, sir. I heard it in the hallway on the way in here.

THE CHAIRMAN. All right. Mr. Secretary, you are now informed.

MR. MANSFIELD. I wasn't sure if it was official. I was trying to get that information.

GENERAL HOWARD. Sir, it was official—

THE CHAIRMAN. All right, let me just ask. Mr. Miller, may I continue?

Something deep inside here is telling me something, that there have been meetings at the table; the CIO, the former CIO, Mr. McFarland, didn't get along too well at these meetings at the table. He tried to perfect some changes. He ended up making a professional judgment to leave. We now have the CISO, who has now resigned. Regarding this memorandum, Mr. Secretary, that you have issued, did the CISO participate in the drafting of this memo, or give input with regard to this memo over security matters it VA?

GENERAL HOWARD. Sir, I am not sure if he was personally involved, but I definitely know his people were. I can get you the answer to that and they—

THE CHAIRMAN. You know, I really can't blame the guy for resigning. If I were the man in charge of security for a department—that is exactly what the Secretary has asked of me—and have not been invited to be at the meeting of the drafting of the security issues on behalf of the Secretary?

Let me ask this, Mr. Secretary: who was in charge to help put this matter together for you?

SECRETARY NICHOLSON. This was a collegial effort between myself, the CIO, the Deputy, the General Counsel, our consultant, Mr. Romley. There were a lot of people involved in this.

THE CHAIRMAN. All right, thank you.

SECRETARY NICHOLSON. But I would say, Mr. Chairman, I would not be surprised if there aren't other people that resign, because the world is changing over there. And these two and I think there might be other people that will resign.

THE CHAIRMAN. Well, I don't doubt that. Mr. Miller's question here—I thank you for bringing this to our attention—but if it is the people of whom are supposed to be perfecting these changes, who are fighting against the culture and they are the ones who are leaving, maybe the wrong people are leaving. I yield back to Mr. Miller.

MR. MILLER. I yield back Mr. Chairman.

THE CHAIRMAN. Dr. Snyder, you are recognized.

MR. SNYDER. Thank you, Mr. Chairman, and thank you for your work on this. I have been unable to attend all the hearings we have had because of the Armed Services Committee has been often at the same time, but I appreciate the hearing.

I had one little detail question, Mr. Secretary. When I arrived today or several of us arrived today at the beginning of the hearing, we had a bit of a circus going on here with you talking into a microphone and holding a mini press conference. In your opening statement you said someone asked you to take the microphone and make some kind of informative statement. Who asked you to take a microphone and make a statement?

SECRETARY NICHOLSON. I don't know. Some person from the press, as my press person was coming down the hall, said "they were going to ask you to make a statement when you step into the room about what has just unfolded with respect to the data."

MR. SNYDER. What is the current status, as I assume you are in the same boat that we—I assume you have one of your letters—

SECRETARY NICHOLSON. I did, yes.

MR. SNYDER. I got one too. I appreciate you sending it to me. What is the status, though, that was mentioned, you know, I guess from Mr. Filner, about credit reporting? You have publicly announced that veterans would have some kind of monitoring of credit reporting, and I expect there are veterans that have relied on that information at some point along the way. Have you made any kind of announcement or decision about where we are at with regard to the announcement you made recently with the credit reporting?

SECRETARY NICHOLSON. Where we are with that, sir, is we are writing the RFP right now, put that out for bids, for the companies that provide that service to bid on. There are certainly three of them: Trans Union, Esperion, and Equifax—

MR. SNYDER. Are you moving ahead with that, or are you under discussion now of not moving ahead with that in view of the fact that the computer was found?

SECRETARY NICHOLSON. That was a question I think was asked the little while ago. You know, a lot has changed this morning. We have been pretty focused on this hearing, but my internal sense is telling me right now that we ought to definitely go ahead with the capability that is out there to analyze data to see if they are being exploited. That's relatively inexpensive. And continue to, you know, to verify and see if the FBI and these people are conducting these forensic

analyses have a high enough sense of confidence that this has not been used, that we need not do it, while having that other screen out there looking to see if anything pops up, and they have a pretty good way of telling whether a collective amount of data is being used.

MR. SNYDER. In the memorandum of June 28, your memorandum, Mr. Secretary, which seems to be very thorough in the way you all put it together, but there is an itemized list of what is delegated. And you say, "this includes but is not limited to the authority to." Give me a few examples of some things that are not on the list, you know, that phrase "is not limited to" ? What are some things that are beyond what is on the list of delegated authority?

SECRETARY NICHOLSON. Could you point to—

MR. SNYDER. Says number two, Delegation, "This memorandum delegates the Assistant Secretary for IT complete responsibility and complete authority for enforcement of information security policies, procedures and practices. This includes but is not limited to the authority to."

What are some examples of some things of authority that you are delegating but is not in this itemized bullet point list?

SECRETARY NICHOLSON. I think that language is somewhat boilerplate-ish in that I intend for this to be expansive or, you know, not to be inclusive, but to be exclusive, to—I want the Assistant Secretary for IT to feel empowered in a broad way, and not a narrow way.

MR. SNYDER. Is there any discussion—I know you have been in the crisis mode here for several weeks. Is there discussion underway, currently with regard to this issue that has come up before, about when and if both the military and Veterans Affairs Department is going to abandon the use of Social Security numbers as an identifier?

SECRETARY NICHOLSON. Yes, we had a lot of discussion about that in this crisis that we have been in. I can't tell you I am too sanguine about it, because you know, to be a veteran you have to come through DoD, and on every dog tag and—I have got an ID card in my wallet, that has got my Social Security number and on it, military ID card—

MR. SNYDER. Yeah, but we are of a different generation, Mr. Secretary—Ms. Herseth and Mr. Michaud—my service number was not my social number—1969, I finished my—I enlisted in 1967 I have a service number that is—I still remember, but is not my Social Security number, and in 1969 the change was made from the Social Security number, and what can be changed one time can be changed back. But I agree there clearly will have to be a coordination, potentially with the military about that, and that maybe something that ought to get—I assume you all are having discussions.

SECRETARY NICHOLSON. We are, and certainly we are not rigid on it. We could deal with the different identifier.

MR. SNYDER. My last question is totally apart from all of this dis-

cussion here which you have been focused on now for weeks. I want to be sure we are not losing track of anything else. What is the number two thing that keeps you awake these days with regard to what's going on with veterans? If you didn't have all this computer business and cyber breaches, what is the number two thing on your list that is important to you and important to this Committee also?

SECRETARY NICHOLSON. Well, I can only be kept awake once, you know, one night at a time, and this has been doing it. I think it is our—the job that we need to be doing for the returnees from the combat area, that we are doing the transition effectively, seamlessly. You know, we have a growing number of trauma patients and—and our polytrauma centers are performing. That is something that I think about a lot.

MR. SNYDER. Thank you, sir. Thank you. Mr. Chairman.

THE CHAIRMAN. Thank you. Chairman Boozman?

MR. BOOZMAN. Thank you, Mr. Chairman. I also was pleased, as the Chairman and Ranking Member mentioned, that you were saying—things like "wake-up call," and "lightning rod," these are truly the kind of rhetoric that I want to hear. And not just the rhetoric, but it looks like you are doing what you need to do to get things in place. The VA has done such a good job of switching over, as you mentioned, we are the model for trying to get our records this way.

I think we are almost missing the forest for the trees though, in the sense that this is a problem in the VA, but it is a huge problem in government in general. And I hope that as you are around those cabinet meetings, envisioning with the President, envisioning with your cohorts in the other agencies, that there is some coordination, that this is a problem that is not going to go away. That as we do a better job of getting our records, and data like this, we are much more in advancement of doing that, versus the security. A few years ago, if you were to take that information home, you would need a van to haul the computer in. A few years before that, you would need maybe even semi loads or tractor-trailers, to get that information home. As you mentioned in your testimony not too long ago, that data, I think, you said five times that data now could be just on, basically a card.

So I guess the question I have got, alluded to you laying awake at night and you are responsible—we are ultimately responsible, in this sense. I am laying awake thinking about lots of different things. Who is the guy now, you are responsible. Who is the guy in the VA that once this settles down—and it will settle down, and, we will get this fixed—what position, who is the guy responsible for moving this thing forward? What position is that? Who is the person in that role now? Who will we look to in the future?

SECRETARY NICHOLSON. It is the Chief Information Officer, and that is Major General Bob Howard, who is the Acting Assistant Secretary for Information, and in a pending confirmation. He has had a distin-

guished career in the military, he has had a rich background in IT, was a math professor at West Point, and is a highly qualified, highly motivated person. We are very lucky to get him, and we got him out of private industry to come in and do this.

MR. BOOZMAN. I guess my next question would be—legislatively, has he got all the tools that he needs to do his job?

SECRETARY NICHOLSON. Well, I think collectively we don't. That is, this agency and I would say probably that about other departments of the government, serving on the President's task force on identity theft. I think that we need some more legislation. I mentioned in my testimony, I think we need to change the teeth for violations of the privacy act and make them comparable to those of HIPAA, because there is a real sensitivity about HIPAA. In fact, when I first came in to this job 16 months ago we were done having trouble getting medical records from the Department of Defense because of HIPAA. And we needed them to treat the people they were protecting.

And they were, you know, they were in good faith on that. They felt that was a problem. We need, I think, some legislation to enable us to get what I call clearances for these people. More background checks, which is also going to cost more money. I think we could use some new law on personnel dispositions, you know, we can debate the disposition of this person that we have debated around here, but I think that managers of these agencies, like I am, need more prerogative. We talked about changing the veterans' ID system, we just talked about it, I think that is something that we ought to look at, and I think that FISMA needs some changes to give more enforcement power to the Chief Information Officers. Like ours.

MR. BOOZMAN. Very good. Well again, we are responding to this crisis. And hopefully the silver lining is, in all this, that we really can, through our Committee, and, whoever else we need to involve, can give you the tools to get the job done.

And then again, I really would encourage you to have an individual who is responsible in the VA. We really need an individual that has significant authority with the administration, to coordinate this among the agencies, because the other side is, we are going to wind up spending, hundreds of millions of dollars on this, probably agency-by-agency versus coordinating—because we all have the same problem. And so I would encourage you, as you have the President's ear, to really push him in that direction. Thank you.

SECRETARY NICHOLSON. Yes sir.

THE CHAIRMAN. Ms. Herseth, you are now recognized.

MS. HERSETH. Thank you, Mr. Chairman. And I thank Mr. Michaud for allowing me to pose some questions in the essence of time for other committees that many of us must get to before they wrap up.

Mr. Secretary, I will just associate myself with the comments of

many on both sides here about appreciating the memorandum, your testimony today. Can you tell me about when exactly the police or the FBI recovered the laptop? Was it just yesterday, do you know precisely the date it was recovered?

SECRETARY NICHOLSON. It was yesterday.

MS. HERSETH. And all the data that we were concerned about was on the laptop? It wasn't an external hard drive as well that perhaps wasn't recovered? It was everything that we thought had been compromised we know have back on the laptop?

SECRETARY NICHOLSON. Madame Congresswoman, most of the data was on the hard drive. But we have both of them, we have the laptop and the hard drive.

MS. HERSETH. And the hard drive, okay. And I am going to submit a question for the record before I have to leave, to all the Under Secretaries that are here, and the Deputies as well, based on some of the questions we have posed over the last couple of weeks to other witnesses on different panels.

But let me ask you this, Mr. Secretary: a few people have asked about the credit monitoring, the fact that we have let veterans know we are going to do this one year of free credit monitoring. And I know that some might contend that things have significantly changed in light of yesterday's development. I don't think so. I would like to think so, but when we have incidents in Minneapolis and Indianapolis, when some of the questions that have gone to whether or not the employee in question here had authorization or not, I have this great fear that there is data floating around out there, whether it was authorized to be taken out or not. And in the case of the Minneapolis case it was last year and you weren't made aware of it until recently.

And I agree with the Chairman. I just think you came into a tough spot; at times you haven't been served well, and I would contend that we should continue and move forward. Even with the cost of offering one year of free credit monitoring, to put people's minds at ease, as you make this ID IT realignment. Would you at least be open today in responding that you will fully consider continuing to offer the one year of credit monitoring in light of these other instances of potentially compromised data, particularly in Minneapolis when it looks like maybe two individuals whose paper files were taken out may be defrauded?

SECRETARY NICHOLSON. Well, so noted, Congresswoman. With respect to Minneapolis, the 66 people there, they are going to get credit monitoring. The 16,500 in Indianapolis, they will get credit monitoring. As to this big thing, I am going to reserve judgment.

MS. HERSETH. But let me just rephrase. You have not made any final decisions as of today that you are not going to continue to pursue the RFP, and put this out to bid, and offer credit monitoring?

SECRETARY NICHOLSON. No, I have not.

MS. HERSETH. I would just suggest to my colleagues on the Committee that there is some potential risk, some huge risk that continues to be out there, and we should also consider whether or not the entire universe of veterans' data that is held at the VA, that one year of free credit monitoring to all of our veterans might be in order.

But anyway, let me just pose this before having to depart: I think now we have the memo that delegates clear authority to the CIO and now that we have contractors that you described, that are going to help move this IT realignment forward; the question that I would pose, and would hope that each under secretary could submit to the members of the Committee, timely, is how do you think things are going to go differently now. I don't want there—none of us want there to be, as Mr. McFarland described yesterday, these disagreements with any of the recommendations for how to go forward with IT realignment, or disagreements with the memo. We are here now. We have the memo. We have the contractors to move forward with the realignment. So how will each Under Secretary do things differently than they did before in ensuring that compliance moves forward, that the recommendations are implemented, and that we don't have inaction in response to disagreements that continue to exist?

SECRETARY NICHOLSON. I think that is a very good question. And things are already happening, and differently, and I mean, I told you that we moved 4,610 IT people out of their, you know, comfort of their present work cocoon into a new department. There is a great amount of uncertainty and anxiety that goes with that, and we are trying to leaven that with the fact that we think we are going to be better off because they are going to become professionals in their own career field which we are establishing.

And that has the full credit and support of the three Under Secretaries, you know, the three operating arms of the VA: medical, benefits, and burials. They are strongly supportive of that. They also of course—I think they would tell you—had a lot of these meetings that we have had, they have been charged to be very, very vigilant. We have the Chief Information Officer, has now, you know, a great deal of authority and responsibility, but they are in the loop as well, when it comes to enforcement of transgressions of their people. And answerable to me on that.

But I think the transcendent point is that there is en route a new culture. And there is a big need for that, frankly, and you know, it is my job to make sure that that progresses and happens.

MS. HERSETH. Thank you, Mr. Secretary. Thank you, Mr. Chairman.

THE CHAIRMAN. Ms. Herseth, in regard to your questions to the Chair, Mr. Secretary, it is worthy of your consideration for an IDIQ contract, whereby you can award a contract based on quantity and

usage. Therefore, you should consider placing this in your budget, while you are getting hold of this one, knowing that we already have some present data losses, whereby a contract can be ordered. You might be able to access this, because I think we are going to have some other breaches, until we can come into full compliance.

And probably that would be my recommendation, rather than just awarding it to everyone. But you are going to have to come up with a budget number and request for proposals, most importantly to put the veterans in good stead.

Mr. Bradley, I thank the gentleman, and I yield.

MR. BRADLEY. Thanks very much, Mr. Chairman, and thank you, gentlemen, and certainly Mr. Secretary, Deputy Secretary Mansfield, for the forthright way that you have answered the questions today, and the leadership that you have shown to try to deal with what has had to have been an extremely difficult situation for all of you personally, and certainly for the 26.5 million veterans.

I apologize if this question has been answered. Like Dr. Snyder, I was at an armed services hearing on the Sarin containers that were found recently in Iraq and trying to be in two places at once.

Did you describe how the computer was actually found, how the FBI—I assume you said was the FBI found it?

SECRETARY NICHOLSON. Congressman Bradley, I cannot detail, because one, I don't know. And two, the FBI, when I talked to them last, which was—well, I talked to the Deputy Attorney General before the starting of this hearing this morning, and there have been a few developments since then, like an e-mail from an FBI spokesman, you know. I don't know if you were here or not, but it said that it appears that this data has not been exploited in any way. We sure hope that is true.

What I have been told is that there have been no arrests made, that this data was provided to law enforcement and that the reward is operative.

MR. BRADLEY. And at least at this point in time, and my last question is, you are reasonably certain, based on what the FBI has told you, that the hard drive was not breached in a way that would have revealed the data?

And how long do you think it will be until you are more certain, and reasonably certain? Or is there no way to even know that at this point?

SECRETARY NICHOLSON. Whether or not you can know this with 100 percent certainty, I don't know. I will tell you what I do know. And I was told by the Deputy Attorney General with whom I spoke just before coming here, and I asked him the same questions that you are asking me about the timing on the analysis by the forensic experts. He said that it will be soon. He also said there was a reason to be optimistic.

So I asked him to follow up and I got no further details, but he did say, on the timing, he did say it would be expressible in days, not weeks. Since we have come here we have gotten this e-mail from this FBI spokesman. So, you know, that leads me to believe that they have gotten pretty conclusive about how they feel about.

MR. BRADLEY. And my last question, when you have determined as conclusively as you are able to conclude okay whether the data has been breached, and the 26 million veterans either have to continue to worry or not worry, are you going to do another letter and inform them of the status of, you know, the information?

SECRETARY NICHOLSON. That's a good question, and I honestly haven't had time to think about it. We have been thinking about the credit monitoring question, but the letter is provoking. I will think about it. Thank you.

MR. BRADLEY. Very good. Thank you.

THE CHAIRMAN. Thank you. Mr. Michaud?

MR. MICHAUD. Thank you very much, Mr. Chairman, for having this hearing, and your continued interest in looking at this issue.

And I want to thank you, Mr. Secretary, in coming before this Committee. I also appreciate the focus you are now giving this issue and your willingness to keep the Committee up to date on the progress that is being made. A couple of questions, and you mentioned something here earlier today in previous meetings that relate to what Mr. Filner had brought up earlier that you are disappointed that you did not fire the employee immediately, that you needed more prerogative.

But looking at the documentation Mr. Filner had presented, it is clear the employee, had home use, he had a license for the program, he had authorization to remove the computer and accessories. It looks like the employee was doing his work. I guess the concern that I have is that in your statement a little earlier, that you need more prerogative, is that an individual who was authorized to work at home is being used as a sacrificial lamb to cover the gross data security problem at VA.

You know, civil service laws exist, Mr. Secretary, for a reason. They exist to protect career civil servants from being political scapegoats. I view this as a leadership failure. The data breach is the fault of VA leadership, for failing to implement the necessary data security measures that time after time after time have been recommended by the Committee, by the IG, and by the GAO. It is the leadership where the failure is at. And I do not think you need any more prerogative to do what you have to with that leadership.

As far as using this one employee as a scapegoat or firing, I think that is more bad judgment after bad judgment. My concern is, what is going to happen here on out for other employees who are authorized to bring work home and are broken into and equipment is sto-

len? It is going to lead to them not actually reporting it. So I do think you have the prerogative, because I believe a lot of this failure is at the top level.

My question is—a couple of questions. Dealing with the $131.5 million that is going to be used for the credit monitoring, and it looks like that might not be used, but if you still have to use it, whereabouts is that going to come from within the VA budget? What programs will have to sacrifice because of the moving of the funds?

SECRETARY NICHOLSON. Twenty nine point five million of that will be a program that come from the VA, Congressman Michaud. And that will come, if it comes, from unexpended funds in the VBA, Veteran Benefits Administration. They are ramping up, but they are—had some savings in there. Many of the hires that they have made have been more junior pay grade than anticipated, so there has been a savings there. Plus, there is some lag in the training cycles, put these people in, that has saved some payroll expenses. And the combination allows us to make that transfer out of there without any diminution of services, or diminution of hiring in the VBA.

MR. MICHAUD. When the budget is put together, are you fully funded for all the positions you are authorized to have, even if they are vacant?

SECRETARY NICHOLSON. Are we fully-funded for all VISNs?

MR. MICHAUD. The head count that the VA has, are those, when you submit your budget, when you get your budget, are those position counts fully funded? Even if they are vacant?

SECRETARY NICHOLSON. In the VA?

MR. MICHAUD. Anywhere within the VA system. If you have head count—

SECRETARY NICHOLSON. If I understand your question right, I think the answer is yes, referring to our VERA allocations to the VISNs; yes, we look at the positions in those VISNs and allocate that money thusly, which is based on the veteran population count, you know. So yes, the answer is yes.

MR. MICHAUD. I only received the memo today, that was handed out earlier this morning. Not having a chance to compare this with what former Secretary Principi had done, I thought, if I remember correctly, what the former secretary did was similar to this. How does what you are doing today differ from what former Secretary Principi tried to do?

And the second part of the question is, in this memorandum have you given all the authority that you are legally able to give over to the information officer?

SECRETARY NICHOLSON. Yes, I have, in answer to the last part of your question first. Secretary Principi issued two memoranda in this regard, that were pretty much disregarded. There was also a disagreement between the Secretary and Secretary's office and the General

Counsel's office about the delegation, and whether the delegation was operative, and effective, and permissible. That is not the case. This is—gone over this very carefully. The General Counsel is in concurrence with this. This is a stronger, clearer delegation of both responsibility and authority. And there is a great amount of command emphasis on this.

MR. MICHAUD. Okay, I don't know if this is a question for you, Mr. Secretary, or Mr. Howard, but as Acting Assistant Secretary of Information Technology, does the Secretary's letter, Mr. Howard, from yesterday, delegate authority for—to you, that applies to you fully, or are there legal limitations, because you have not been confirmed by the Senate?

SECRETARY NICHOLSON. I will go, then I will ask Bob Howard if he would like to comment. I need to point out that on the enforcement part, with regard to people who are not in his command, that belongs to the Under Secretary. So they, that has to be a communication between the CIO and them. And I am looking to them, then, to do the enforcement. So that is a power he doesn't have from this.

With that, I would ask him, do you have anything to add, Bob?

GENERAL HOWARD. Sir, I have the letter from the Secretary designating me Supervisor of the Office of Information and Technology, and to do what I need to do, and that is what I intend to do.

MR. MICHAUD. Even though and you haven't been confirmed by the Senate as an Acting Assistant Secretary?

GENERAL HOWARD. The letter gives me all the authority I may need.

MR. MICHAUD. Thank you. My last question, Mr. Secretary, deals with an issue that actually came up at one of the other hearings we had earlier from a former employee of the VA when you look at the failing grades, so to speak, of the agency. When you deal with security and data issues, that former employee thought that VA failed I think 16, or can't remember how many areas, and that there should be no bonuses given out to the folks who are within the agency. You have the authority to give bonuses. I don't know if you heard the testimony on this issue, but, what are your comments on that?

SECRETARY NICHOLSON. I didn't hear that testimony but I guess whoever you are talking about, I agree with and I testified to that in my opening statement. I think that is another way to put some teeth into this, into this cultural change that we need to make, as it will pinch them in the pocketbook as well.

MR. MICHAUD. So is it your intention that any time, if the Inspector General comes up with a report, and you have failed, that you will not be giving any bonuses?

SECRETARY NICHOLSON. It is my intention to look at each of those cases with that in mind, yes, sir.

MR. MICHAUD. So they could fail, but you still might give bonuses.

SECRETARY NICHOLSON. Well, it is hard to imagine doing that if they failed, because I believe, you know, in performance pay and in performance reviews. And bonuses are also an incentive—well, not also, they are an incentive. But in this case, they are going to become sort of a negative thing if people are not performing, and giving this the attention that it needs.

MR. MICHAUD. Thank you very much. I yield back, Mr. Chairman.

THE CHAIRMAN. Thank you very much. Ms. Berkley, you are recognized.

MS. BERKLEY. Thank you, Mr. Chairman, and I will be brief. I had a series of questions, but I would like the opportunity to review the testimony, because I wasn't here during a lot of the questioning, and with a little effort on my part, some of these questions may have already been answered. And whatever is left, I would like to submit, if that is all right.

THE CHAIRMAN. Ms. Berkley, you may submit questions for the record. We will be responsive.

MS. BERKLEY. Thank you. And if I can just make a quick statement, I first welcome all of you. We are not strangers to each other and we have worked very well together on behalf of the veterans in my community for quite a while now. I think we have been very fortunate and hopefully we have averted a crisis here. And I am hoping that it will serve as a wake-up call, not only for the VA department and for all of us, but for the other agencies and departments within our government, that they need to start looking at these systems and ensure that the privacy not only of our veterans but of all Americans are protected.

And I think this is an important first step for us. I have been very critical of you, Mr. Secretary, and I think you know that. When you were here earlier in the year to present the budget, I didn't think that after a year of being in your position that you were as engaged as I would have liked to have seen you and as knowledgeable about what was happening in your department as I think you needed to be, and I believe I said that at that time.

I also think it is important to compliment as well. The difference between now and a few months ago is quite dramatic and I am very happy to see it. I think as I mentioned, this is a wake-up call for all of us, but the burden of your position has fallen on you and I think you have picked up the gauntlet, and understand the importance of what we are doing here collectively.

SECRETARY NICHOLSON. Thank you.

MS. BERKLEY. I also want to thank you for that and I suspect—I know that between Mr. Filner and Mr. Buyer, we will be watching, and hopefully, this will not be the VA will not be an embarrassment for any of us; quite the contrary, it is going to be a shining example of what we can do well in government to protect the people that look

to the United States Congress and the United States government to have their needs met.

So I am looking forward to working with you on this. And I will submit whatever questions you haven't answered after I have had an opportunity to review your remarks to other questions. So thank you very much.

Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you very much. I would like to ask an open question to all of the witnesses. Does anyone here have knowledge of any other data breaches within the VA other than what has been presented in Maryland, Minneapolis, and Indianapolis?

MR. MANSFIELD. Yes, sir, I do.

THE CHAIRMAN. Yes, Secretary Mansfield?

MR. MANSFIELD. Mr. Chairman, yes, I do.

THE CHAIRMAN. All right, where?

MR. MANSFIELD. There is a newly instituted weekly report that comes forward that identifies the incidents across the system. Some of it is historical and includes the two that you have just mentioned. It just got started this week—sorry, it started three weeks ago. It goes down in the Office of Cyber Information Security. The operations group, they are the ones that with the new collection of all the ISOs that do a national group, or a centralized group under the office of IT, that are now reporting through the national system.

So that report just started, and one of the things we have obviously learned this morning is that there isn't a part of it that requires notifications as you mentioned. That's part of what we had to work on as we bring folks in to help us redesign the system on a national basis.

THE CHAIRMAN. All right, and where is the additional data breach?

MR. MANSFIELD. Sir, we have a whole list. Most of them are small, some of them are pending information, and the most recent—

THE CHAIRMAN. While the Deputy Secretary is reviewing the list, Mr. Secretary, have you been informed of this list?

SECRETARY NICHOLSON. I know that we are making this list, we are keeping this list, we just started this. And I have been presented with this list, I don't know that I have this copy that Gordon is reading from.

THE CHAIRMAN. All right, let me ask this, before we go too much further. This list would contain how many incidents approximately? Is this pages?

MR. MANSFIELD. Sir, I would have to—one, two, three, four, five, six, seven, eight, nine, 10. And I could make the point that these cover the waterfront. For example, this one talks about potential unauthorized access to information, and it goes down and talks about this case can be closed out as the contractors were authorized access to sensitive information, so—

THE CHAIRMAN. All right. I think what we are doing here is helpful,

because what you are seeking, Mr. Secretary, is a process of open disclosure. Because what you have got is a team, and you have to build that esprit de corps. And if somebody makes an error, you need to know about the error because we need to make sure we take care of veterans and then that it is corrected.

So my purpose here is not to go through all these. I want to know what our vulnerabilities are, what is out there. I would like to speak with you offline about many of these because some of them you may not want to discuss. I don't know where they are in the process. I yield to you, Mr. Secretary.

SECRETARY NICHOLSON. I think that, Mr. Chairman, if you like it would seem to me we could provide this report to you and the Ranking Member if you want it, if you want to see that on a weekly basis. I mean, you know, we are trying to be really sensitive. Here is one where, you know, an employee may have taken sensitive information home on a spreadsheet contains some information about medications. You know, we are try to err on the—

THE CHAIRMAN. You know what, I can even see a lot of this happening. So in your opening testimony, you say to us that you are going to check all laptops, that you are going to make sure that they are all secure. Have you granted any waivers to that policy?

MR. MANSFIELD. Doctors.

THE CHAIRMAN. Doctors?

SECRETARY NICHOLSON. No, we have not granted any waivers to checking, but doctors who deal with patients from home will have to be able to continue to do that. We do know that. But that doesn't exempt them from a data call.

THE CHAIRMAN. All right, going back to this issue on the budget for the moment. It appears that until you are able to perfect your federated model, as you move to centralize your IT management systems, we are going to continue to have vulnerabilities. As the culture begins to change, it is highly possible that we will have some future data breaches. There is a human element.

So Mr. Secretary, I would ask of you to work with OMB. You work with OMB with regard to your potential budget supplemental, the $160.5 million. It appears that that number will now change. But it appears that some monies will need to be accessed.

My hope is that in your communication with OMB, I don't want OMB to say to you, Mr. Secretary, "You are to take this out of hide," and "out of hide" would be, you know, FTE for personnel with regard to claims processing, and the other painful decisions or judgments that you have to make. So I would hope that you would communicate with OMB and the director that with regard to these monies that were offered up, when they said to you "that last $29 million had to come from you," that was the last part, and we ought to be able to access the monies with regard to this account for you to do one of

these ID IQ contracts, and we could access as we proceed. Would you concur that that would be a good initiative?

SECRETARY NICHOLSON. Well, I absolutely concur, and, you know, of course had those conversations with OMB on that subject. Yes, sir.

THE CHAIRMAN. All right, very good. With regard to lines of authority, General Howard is going to directly report to whom?

SECRETARY NICHOLSON. Direct report to me.

THE CHAIRMAN. To you?

SECRETARY NICHOLSON. Yes.

THE CHAIRMAN. Does he have dotted line to the deputy, or just a straight shot to you?

SECRETARY NICHOLSON. A straight shot to me, with a dotted line to the Deputy.

THE CHAIRMAN. Okay, now as we proceed on the implementation of your federated model, our milestones or benchmarks, performance measures, have these been, are they in place, with regard to your Under Secretaries, so that they can provide the leadership that down the chain, that your initiatives are being implemented and executed?

SECRETARY NICHOLSON. The answer is generally yes, in that we have, you know, a very good consultant in place helping us with that, and we have, as I said now two or three times this morning, we have already detailed those people out of their old existing organizations into this detailed status of the new IT organization. And then come October 1st, the beginning of the fiscal year, they will be formalized in that. That of course is a major benchmark. And we have several others in this perk chart that we are following to do this with.

THE CHAIRMAN. All right, we will follow that with you.

SECRETARY NICHOLSON. I am sure you will.

THE CHAIRMAN. Let me turn to your Under Secretaries if I may. Dr. Perlin, with regard to our patient medical records, what assurances can you give veterans today that as we perfect the federated model, that these records are secure?

DR. PERLIN. Mr. Chairman, the electronic health record is a great advance in security over paper. Unlike paper, there is an audit trail. But with the advances in the department, with the leadership that will occur in cyber security with the end-to-end encryption as was discussed here in previous hearings, the security that already exists will be enhanced.

Unlike the tragic event that recently occurred, the electronic health records are not transportable in bulk. And so that is in itself one very important assurance. And when they are looked at or accessed, there is an audit trail of who was there, and with that we can know why.

THE CHAIRMAN. All right. Before I yield to Mr. Filner, we had painfully learned here over the past few weeks how Mr. McClain's memo was interpreted. So we are very clear that with regard to authorities of enforcement of the Secretary's policies, that it rests with the under

secretaries, that the so-called "F" belongs to you.

So what that means is, as I turn to the Secretary and say "you are not being served well," I return to the under secretaries and say it is also your moment of leadership. So please advise the Committee right now, and we have the three of you testify, as to what are you doing to ensure veterans' records are secure?

Secretary Tuerk?

SECRETARY TUERK. Well, thank you for that opportunity, Mr. Chairman. As you will see in my prepared testimony, we have taken a number of actions, we are in the midst of executing a number of actions, and we have a number of actions planned for the future, essentially all leading toward the same goal.

These actions emphasize my commitment to assuring that veterans' privacy is respected and protected. They reinforce the necessity for all of our employees to understand their obligations in detail with respect to these issues, and they proceed towards implementing, within our internal organizational assessment process, a more penetrating review and self-assessment of compliance with those requirements so that we can assure accountability of the people within the National Cemetery Administration. Everything I have done with respect to this issue has been aimed towards those ends.

THE CHAIRMAN. Dr. Perlin?

DR. PERLIN. Mr. Chairman, thank you as well for the opportunity to comment on this. And I want to say first and foremost that I fully support the Secretary's plan—a real opportunity to work on developing what we hope will indeed be the gold standard for information and privacy, not only in government but certainly also in health care. This week is an important week; as the Secretary mentioned at the beginning of the testimony, this is Security Awareness Week, and we are pleased that VHA took the lead in authoring the activities in support of the Secretary's plan for the different events during Security Awareness Week.

Because however hard we make the hardware, and however tight we make the software, it ultimately comes down to the warm-ware, the people, and that is why we believe that today, through this week, that security awareness has to be the first part, to make people understand the need to operate with the information necessary to do-, but transport or access the minimum information necessary to do-their jobs. So at this very moment, I am literally on a broadcast throughout the system, instructing the VHA employees on the importance of operating with vigilance and diligence, and the protection of secured information.

We support Bob Howard and the activities that he will bring forward in terms of hardening, the biometrics that limit the access, and prevent, and preclude inappropriate access. Because while this occurred in an area totally, totally unrelated to health records, we em-

brace that this is a wake-up call and an opportunity. We support anything that comes forward in the Department in terms of encryption. We believe that can enhance our ability to safely serve veterans. We are inventorying all of the data sets and inventorying all of the assets throughout the system again to ensure that where it exists, there is a need to know; that people understand that that is a privilege in the process of serving veterans. Thank you.

THE CHAIRMAN. Mr. Aument?

MR. AUMENT. Yes, Mr. Chairman. At VBA, we have undertaken a complete review of all of our policies and procedures governing access to information and access to VBA systems in particular. We have rules of behavior that anyone who wishes to gain access to a VBA business system, whether that be a VBA employee or others who may be authorized access to VBA systems, such as veterans' services organization representatives, we require that they first of all undergo the cyber security training that all employees must undergo, and that they read and understand and sign our rules of behavior.

We have acquired encryption software that we are going to be applying to all laptop computers in the Veterans Benefits Administration. We have had all of those laptop computers returned to the home office by their employees. Once general counsel has given us a green light to proceed to install that software, we will proceed to ensure that all laptops are encrypted. We have taken steps to make sure that all of our employees within the organization have completed both the cyber security and privacy training, that are to be completed by tomorrow.

We believe that we have taken very strong steps. We have also reviewed the agreements that we have in place to provide outside entities information from VBA systems. That includes entities both within the department and external to the Department of Veterans Affairs. And we are making sure that those are current, they are still needed, and that they bring with them all of the access controls that are appropriate for the data that is being provided.

THE CHAIRMAN. Thank you. Mr. Filner?

MR. FILNER. Thank you, Mr. Chairman. Let's wrap up this long hearing for all of you. Mr. Buyer asked the folks in the front row. Let me just get the folks right behind you, if you would give the microphone to Mr. Whitney. Your position, Mr. Whitney?

MR. WHITNEY. I am the office system administrator, privacy officer, and security officer.

MR. FILNER. And you help people with routine IT problems, I take it?

MR. WHITNEY. Day-to-day, yes.

MR. FILNER. And would you help people load up their computers for their software, their accessories, say, if they worked at home?

MR. WHITNEY. No, I do not load up home computers. I would provide

the appropriate software once they have been approved for home—

MR. FILNER. Well, I am not talking about a home computer. Say you have an office laptop that would be taken home to do work at home.

MR. WHITNEY. Yes, if it was designated for that, that would be me.

MR. FILNER. And people do that, right? They take work home? They are authorized to do that?

MR. WHITNEY. Yes.

MR. FILNER. And so you would help load up the software if they required it.

MR. WHITNEY. If it was necessary, yes.

MR. FILNER. Okay. I just wanted to see how that was working. And Mr. Duffy, your position right now?

MR. DUFFY. I am presently the principal Deputy Assistant Secretary for Policy and Planning.

MR. FILNER. And as of tomorrow?

MR. DUFFY. As of tomorrow, I will officially retire from the Department of Veterans Affairs.

MR. FILNER. How long have you been with the department?

MR. DUFFY. Been with the department 34 and a half years.

MR. FILNER. That's a long time. Thank you for all that work.

MR. DUFFY. Thank you.

MR. FILNER. When someone has software, a software license that authorizes home use of the software, that is intended for office work, right? That is the purpose?

MR. DUFFY. That is correct.

MR. FILNER. And so, this employee who had that authorization, what was exactly he doing?

MR. DUFFY. The individual was a senior data analyst, a statistician. He worked on a variety of different analytical projects, including things like the development of the next national survey of veterans.

MR. FILNER. And that is what he was working on when this—

MR. DUFFY. That is my understanding. That was one of the issues that he was working on at the time of this particular tragedy.

MR. FILNER. Mr. Duffy, We wish you well in your retirement.

MR. BOWMAN. Thank you.

MR. FILNER. Mr. Bowman, you are the Chief of Staff, give me an English definition of that?

MR. BOWMAN. Well, sir, as the chief of staff—

MR. FILNER. For the Secretary?

MR. BOWMAN. For the Secretary, yes, sir.

MR. FILNER. And how did you come to know about this tragic situation?

MR. BOWMAN. I was made aware of it initially in a conversation with Mr. Duffy on the 9th of May.

MR. FILNER. Did you think there was a sense of urgency?

MR. BOWMAN. I felt that there was a sense of serious concern, based upon how it was described to me as the potential for the loss. But there was still some doubt as to exactly what was the magnitude of the loss.

MR. FILNER. And how far do you actually work from the Secretary?

MR. BOWMAN. Sir?

MR. FILNER. How far is your office from the Secretary's office?

MR. BOWMAN. Maybe 75 feet.

MR. FILNER. And I assume you talked to him many times during the week, after you knew about this?

MR. BOWMAN. Well, sir, there were two days—I have open access to the Secretary.

MR. FILNER. I still can't figure out, as a chief of staff, why you didn't tell him about it earlier than you did.

MR. BOWMAN. I can tell you right up front that me not telling him I regret at this point. But when I became aware of it on the ninth, I felt it important to gain a little more information, and I asked Mr. Duffy to provide me that information in a memo. The concern being, with a greater awareness of what might be the magnitude of the loss and the kind of information that may be missing, it would help define what might be the approach the department may take in addressing it.

MR. FILNER. Has the Secretary expressed regret that you didn't tell him? I mean—what is going to happen differently in that relationship and knowledge that comes to you, based on this?

MR. BOWMAN. Well, one thing that has happened differently is that as I become aware of anything that would be important to the Secretary, I report it and obviously I have to apply some sense of judgment to that, I exercise very open access with the Secretary and with the deputy.

MR. FILNER. Thank you. I appreciate that. You know, we have the luxury of asking you in hindsight, and I realize that. But it looks to me, there were serious lapses of judgment, and not sufficient appreciation of the effect on the veterans and the fear that was propagated to everybody.

I think all you at the top failed us—not failed us, failed the veterans. Again, I mentioned at other hearings, I had a recent election, so I was talking to a lot of people in the last month, after the theft was known. There was incredible fear, and a sense that veterans didn't know how to handle this, and they weren't getting the help, or assurance that they were going to be helped, and I think you all have to examine that whole process. I mean, you got to have—some of you military guys, in your debriefing, or after action reports, you got to go over this and see what happened.

I am not going to just say everybody ought to be fired—I have said

some things like that in the past—I think all of you want to serve the veterans. But this is a serious lapse and you have to figure out why it happened and make sure it does not happen again. You all have to work on that, and let us know how that is solved, because the folks outside are really, really afraid.

Lastly, Mr. Secretary, I think you are appropriately still leaving open the need for credit monitoring. You have put a lot of emphasis on credit reporting as your proactive thing. The testimony that we have had from these experts—and it sounds like you have had similar conversations, because of some of your answers—it may be more important—one, I would have, if this thing was still an open question today, I would emphasize insurance, some sort of insurance policy for loss, because it is cheaper and it is much more assuring. Any credit changes, if this was a professional job, would not be apparent for a year or so. So it may not do any good to monitor.

And the RFP that you are still working on, getting a sense of was there any identity theft based on analyses of different databases, is far more important and a lot cheaper. At least one company that testified said they would do it free for the first year. So I think this is a matter of judgment still. And I don't think that you have to assume that just credit—everybody is saying "credit monitoring." That doesn't sound to me like the answer that you need, especially at this point. The "screen," as you called it, between a certain set of data and what could have happened to it is far more important, because it will show up on credit later.

I still don't understand why we have a lot of experts here that never even talked to you. I think you should have called them first. I still can't figure out why Mr. McClain doesn't talk to other general counsels about interpretation of FISMA. As several people said on both sides of the aisle, the coordination here with other departments is absolutely vital. And if Mr. McClain was the only one who said that you had to interpret FISMA this way, versus 10 others, that should have led to some questioning in the department, why is he the only one saying this?

These are just some thoughts I have from someone who has been critical. I am trying to say, take this seriously and show us that there have been some results and some self-critical judgment. Thank you, Mr. Secretary for sitting through all this. If you have any final thoughts, please—

SECRETARY NICHOLSON. The only one right now I would say, Mr. Filner is, I agree with you, I think we should pursue the, you know, the data screen on this population, just as a belt and suspender, you know, at least, and it is not very expensive. And the question of then credit monitoring in my mind right now is still open.

THE CHAIRMAN. I thank the gentleman. Mr. Aument, before I conclude, I need to go back because I have been pondering one of your

responses and this deals with the issue about the laptops and making sure all the laptops are secure. So, you went out into the field and asked for everybody to bring their laptops in and "let us check them and make sure they are properly encrypted," or have the right software on them?

MR. AUMENT. That is correct, Mr. Chairman. We have had all the employees, those who by nature of their positions have to be working away from the office; visiting schools, appraisers, fiduciaries, we have had them bring their laptops back to their home regional office.

THE CHAIRMAN. What was it that you needed, that you have to get permission from general counsel to do what?

MR. AUMENT. This is the lawsuit that has been filed, that was requiring us to leave the machines intact while the litigation was proceeding. So I believe General Counsel can answer that much better, but we were asked not to make any changes fundamentally to those machines until that issue had been resolved.

THE CHAIRMAN. Well, this is a rather bizarre situation. If we have veterans' groups filing a lawsuit, for them to think they are going to act on the interest of veterans, and the lawsuit now is to the detriment of veterans. I am disappointed, and I am also most hopeful that these organizations would dismiss that class-action lawsuit. This is not necessary, and I am most hopeful that these organizations will direct their lawyers to take appropriate action to do so. It is hard for us to work through this, work with you, Mr. Secretary, perfect change and take care of veterans, if we can't do so because of a class-action lawsuit. Is this also occurring with you, Secretary Tuerk, and Secretary Perlin? Does the same apply to you with your laptops?

DR. PERLIN. Yes, Mr. Chairman. We understand that from General Counsel, that there is effectively an injunction precluding the sort of actions that we would all want to take. I would turn to our General Counsel for additional elaboration.

THE CHAIRMAN. What has the court directed you to do or not do, Mr. McClain?

MR. MCCLAIN. Mr. Chairman, really, there are two separate issues. We have three class-action lawsuits that have been filed. There was a TRO that was issued last Friday in the Eastern District of Kentucky, and will be heard tomorrow at 2:00 o'clock in the afternoon. And the issue there was communicating with potential members of the class, and credit monitoring.

In one of the other cases, there was a very strong letter from the plaintiff's counsel saying that he had heard about the Secretary's plan for the security awareness week, which included one of the items being the security of the laptops, to ensure that things were supposed to be on it were, and were not supposed to be on it were taken off. They sent a letter saying, "we believe that this would be destroying evidence, or tampering potential evidence in the lawsuit," and therefore

our attorneys at DOJ recommended that until we can get the court to rule, that we not do anything with the laptops. So it is a delay in doing this with the laptops; it is not a moratorium.

THE CHAIRMAN. So now we have a Secretary and under secretaries seeking compliance, and they can't do so to secure their systems because of class-action lawsuits. Is that what you are telling me?

MR. MCCLAIN. Yes, sir.

THE CHAIRMAN. That is a sad state of affairs. Now we have got the plaintiff's bar involved. Well, wow. Mr. McClain, the Department of Justice is litigating your defense?

MR. MCCLAIN. Yes, in all three cases.

THE CHAIRMAN. Have they filed for summary judgment in all three cases?

MR. MCCLAIN. That is under consideration right now, sir. We have made no appearance yet in these cases.

THE CHAIRMAN. Given that there is no evidence of damage—you have got a class that has been certified, but yet no evidence of damage, this ought to be an immediate summary judgment. I yield to you, but I think we are certainly—

MR. MCCLAIN. We are certainly considering it, sir.

THE CHAIRMAN. Yes. Well, I would encourage that, Mr. Secretary. We need to get on, make sure this is secure. This is unprecedented in the history of the VA, and you know that, Mr. Secretary.

And I laud your leadership. You have had to take control of this, and you have done that. When I said it was a moment of your leadership, you have stepped forward. And you are off the heels and on the toes. And I think you are sending the right message, not only to the deputy secretary. He gets it, and so do your under secretaries, by their testimony here today.

And Mr. Howard, I do not understand, perhaps, why your cyber security man was not in the room in the drafting of the directive. Perhaps that was your choice, but with this memorandum you have been empowered. It appears that you are about to be embraced to perfect these changes.

Taking advantage of the widely felt impetus for change, as you spoke, Mr. Secretary, I am most hopeful this will yield the vast and crucial improvements necessary in your department, and we will continue our oversight. And I want to thank you, and we will work with you with regard to these budgetary matters.

This hearing is now concluded.

[Whereupon, at 2:11 p.m., the Committee was adjourned.]

APPENDIX

STATEMENT OF HONORABLE CORRINE BROWN

House Committee on Veterans Affairs
Full Veterans Committee Hearing relating to
the Data Security Breach at the Department of Veterans Affairs
June 29, 2006; 10:30 am
334 Cannon HOB

Thank you Mr. Chairman and Mr. Filner, for the bipartisan manner you have conducted these hearings.

As we enter the Independence Day celebration, it is incumbent upon us to remember who we are here for. We are here for the veterans. The veterans who sacrificed so we can enjoy the freedoms we so cherish.

Secretary Nicholson, you have let our nation's veterans down with this security breach.

You are the captain of the ship and you are responsible for the actions of your employees. You are quick to take credit when there is positive news. This is your responsibility.

You inform the press before you inform this Congress regarding the plan for "credit monitoring" for the affected veterans.

$160.5 million for monitoring with $29 million taken from VA funds budgeted in 2006 to cover personnel costs at the Veterans Benefit Administration.

$131.5 million would be reallocated from other areas of the White House budget. I understand that money is to come from food stamps, student loans and trade assistance for farmers. It is very important to pit veterans against

farmers. I applaud you making this data theft a political issue.

I don't trust you. Saying that other areas will pay for your mistakes is unlikely. Extra money is not there. We have been voting for the last month on appropriation bills that are too austere.

There is no extra money.

You also say that your "first priority was to take all actions necessary to protect

veterans from harm and to assist in law enforcement efforts."

Your first priority should be to stop this from happening.

Congressman Tom Udall (NM-3)
House Veterans Affairs Committee
Final Hearing on VA Data Loss
June 29, 2006

Mr. Chairman,

For five weeks, this committee has strenuously studied the VA data loss of May 3rd to determine what happened, who is responsible, and what must be done to mitigate the situation and ensure similar incidents are prevented in the future. I think many of these questions have been answered, and I look forward to working with the Chairman and Ranking Member to draft comprehensive, bipartisan legislation to further this committee's goal to better securing and protecting all personal information utilized by the VA, and to ensure that data management finally becomes a priority for the Secretary and others.

Nevertheless, Mr. Secretary, the question remains of why, for three years, the VA employee was able to take home the information on 26.5 million veterans and 2.2 million active duty and reserve service members, with permission from his superiors as we recently learned, and without any concerned being expressed by anyone throughout the VA hierarchy. What continues to plague these hearings is the overarching issue of a culture of apathy and the entrenchment of status quo at the VA. You must focus on these fundamental issues if there is to be any positive change. You must focus on altering how the VA and every single on of its employees approach the mission of serving veterans. Otherwise, any other modifications will be ineffectual. The best policies and procedures are meaningless if they are not implemented and enforced, and this will happen if the culture surrounding the VA does not change.

In this committee, our oversight of the VA is essential to ensuring veterans are not mistreated. We must continue to hold hearings on these issues to monitor the progress the VA has made in protecting data.

Thank you, Mr. Chairman.

Office of Congressman John Salazar
Opening Statement
House Committee on Veterans' Affairs
Full Committee Hearing
June 29, 2006

- Mr. Chairman, Mr. Ranking Member I once again thank you for holding this hearing today and the previous four hearings we have had addressing the May 3 theft of a laptop from a VA employee's home.

- Everyone in this room is well aware of the situation we will be discussing here today.

- This theft has opened three very important issues for this committee to address:

- The first and most pressing is the protection of the identities of the 26.5 million veterans and their spouses as well as the 2.2 million active duty military personnel whose personal information was compromised.

- Mr. Chairman, I have introduced HR 5588 – the Comprehensive Veterans' Data Protection and Identity Theft Prevention Act of 2006.

- This comprehensive bill will take significant strides towards protecting the identities of those whose personal information has been compromised.

- Specifically, Mr. Chairman, the bill provides for free credit monitoring and an addition free credit report;

- It also would allow veterans to issue free fraud alerts and one free credit freeze on their account.

- These measures alone would help veterans protect themselves.

- The bill also includes provisions calling on VA to promulgate rules for IT security and to establish an Ombudsman's office to assist veterans who are victims of the data breach and identity theft.

- The second issue that the data theft has brought to light is the so-called culture of indifference within VA regarding the implementation of comprehensive IT security initiatives within the Department.

- Through the previous four hearings this Committee has held, we have heard of the systemic problems at VA that contributed to this VA employee taking sensitive information home with him.

- There is a lack of structure, authority and will within VA to make the changes necessary to ensure that data stored there is safe and secure.

- It troubles me greatly that both the IG and GAO have called upon VA to make changes to its IT security policies.

- In addition, this committee has held multiple hearings on this issue and has urged the VA to change its policy.

- I stand with the members of this committee who will call on VA to centralize authority and responsibility for IT security.

- It is unbelievable that a memo has been in draft form for over three years moving from department to department, agency to agency each passing the buck for IT security.

- Lastly, this theft shed light on the lack of a clear communication structure within the Department for the notification of Administration officials, Congress and the general public.

- Congress was informed of this theft 19 days after it occurred.

- This is unacceptable.

- I hope with centralized authority and accountability for data security, communication is more effective and efficient.

- Mr. Chairman, Mr. Ranking Member I again express my thanks for holding this hearing today.

- I look forward to hearing from the Secretary and asking him some tough questions.

STATEMENT OF

WILLIAM F. TUERK

UNDER SECRETARY FOR MEMORIAL AFFAIRS

DEPARTMENT OF VETERANS AFFAIRS

BEFORE THE

HOUSE COMMITTEE ON VETERANS' AFFAIRS

JUNE 29, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for the opportunity to provide an overview of the actions that the National Cemetery Administration (NCA) has taken, is taking, and will take to ensure that sensitive personal information of veterans and their beneficiaries is safeguarded.

NCA IT INFRASTRUCTURE

As background, security has always been a very important part of NCA's Information Technology (IT) architecture. We have incorporated best practices from both the public and private sectors into our system, network, and application designs, and our ongoing policies and procedures. With guidance from the Department's Office of Cyber Information and Security (OCIS), NCA has pursued a strategy of continuous improvement for the security of its information systems. We have standardized policies and procedures governing information access requests, auditing, and rules of behavior. These policies and procedures apply

to all NCA employees, and to non-NCA employees who are granted access to NCA systems and data.

NCA has a centralized architecture for its information systems. All data is housed at the NCA's Regional Data Center in Quantico, Virginia and at NCA's IT "backup" site in Culpepper, Virginia. Access to the system is provided through one of two portals: via NCA's "in-house" data network; or via VA's Virtual Private Network (VPN). NCA staff, including field staff at NCA's 123 national cemeteries, access the "in-house" NCA data network directly in the course of their day-to-day activities. VPN access is used primarily by non-VA entities, *e.g.*, State Veterans Cemeteries or Department of Defense or Interior national cemeteries, to whom we have made NCA management systems available to facilitate their cemetery operations. Both access methods require a user ID and password to authenticate to the network and a separate user ID and password to access specific information systems.

As you are aware, VA IT security policy and oversight responsibilities have been centralized under VA's Chief Information Officer; the VA Office of Cyber and Information Security now has Department-wide responsibility for all IT security. Subject to the supervision of VA's OCIS, NCA implements its IT security policy and procedures for field activities by means of a three-layer organizational assignment of responsibilities. Cemetery Directors are responsible for the execution and oversight of IT security policy and procedures. Memorial Service Network (MSN) Offices provide oversight of cemetery

compliance with IT security policies and procedures. The NCA Data Center provides the technological support that implements IT security. All NCA Data Center employees and NCA Headquarters IT staff were detailed to the VA Office of Information and Technology on May 1, 2006, as part of the implementation of the VA IT Federated Model. They will be permanently assigned to that office on October 1, 2006.

Staff at NCA's Data Center centrally control the standard configuration of servers and NCA desktop and laptop computers. They deploy updates automatically -- including security patches and virus protection updates -- to maintain quality assurance and security. Before a server or workstation is connected to the NCA network, the device is loaded with a standard operating system and security software package, and the registry is locked to prevent any unauthorized modifications.

NCA provides data to numerous VA elements. For example, it provides "first notice of death" information to VBA. With respect to such intra-VA requests for data from NCA information systems, NCA has in place a formal process for accepting and reviewing requests for data extracts from NCA information systems. The information request must be cleared by the Deputy Chief Information Officer and presented to the Director of NCA's Data Center where it is documented and approved in NCA's helpdesk tracking system. In very limited and unusual circumstances, NCA also provides information to elements outside

of the VA, usually in response to Freedom of Information Act requests for non-sensitive information.

NCA also has a secure technology solution in place for individuals, *e.g.*, State Cemetery employees, requiring access to NCA systems from outside of VA. That solution requires external users to access NCA systems through the One-VA Virtual Private Network (VPN). The VPN allows remote users to access VA systems in a secure environment. NCA systems limit access from the VPN to NCA applications only. That is, "outside" users allowed access to the VPN by NCA cannot "roam" within VA's VPN.

All users authorized to access VA systems are required to sign approved rules of behavior. These rules of behavior bar the misuse of government systems, the mishandling of sensitive data, and unauthorized disclosure of sensitive information. They also specify, in the case of Federal employee access, that disciplinary action up to and including termination of employment can result from rules of behavior violations.

NCA completed the Federally-mandated certification and accreditation (C&A) of its IT system applications in October 2004. A second independent C&A of our systems will be conducted in FY 2007.

TECHNICAL AND POLICY CHANGES MADE, AND ANTICIPATED, SINCE DATA LOSS INCIDENT

I want to assure you and our Nation's veterans that the recent data breach did not include any NCA records, nor were burial and memorial services for our veterans and their families disrupted. To ensure that our systems will not be compromised, we have undertaken a number of actions based on a thorough review of our current information security processes. This review, which was equivalent to a DOD safety review stand down, dictated the following courses of action:

Actions Completed

- I have disseminated a memorandum to all NCA employees reiterating NCA's privacy and security policies and practices.

- NCA took measures to assure that all employees complete annual refresher training on both Privacy and Cyber Security Compliance by the end of this week.

- We have completed an NCA-wide accounting of employees accessing sensitive information via automated systems.

- NCA has reviewed the formerly-existing roster of persons having VPN remote access. Based on this review, a number of accounts have been deactivated or deleted.

I established a new requirement that Privacy Coordinators be appointed at every NCA facility that is physically separate from NCA Headquarters to assure that all employees, volunteers, and contractors are aware of their respective roles in safeguarding privacy information.

- We have reviewed and reissued NCA's comprehensive Automated Information Systems Security Directive and Handbook to ensure that NCA information security policies and guidance are current.

Actions Under Way

- NCA is strengthening its Organizational Assessment and Improvement self-assessment guide to ensure more thorough and probing Security and Privacy Reviews are conducted at each cemetery.

- NCA is reviewing the need for the storage of paper records at its cemeteries. I anticipate that we will refine policies and enforcement mechanisms for sensitive document storage.

- NCA is currently reviewing its practices with respect to non-NCA access to NCA systems via the VPN network to ensure that only persons with a "need to know" gain access and to ensure that such persons comply with VA rules of behavior.

- All NCA facilities are currently participating in the Department's IT Privacy and Security Awareness Week.

- NCA is developing a Policy Directive stating requirements for collecting and retaining sensitive data, to include prohibitions on sharing data with third parties.

Future Actions

- NCA will develop a Policy Directive to define sensitivity level designations for all NCA positions.

- NCA will order appropriate background investigations for employees having access to sensitive information.

- Consistent with Department policy, NCA will develop a specific Telework Policy and require NCA workers to agree to VA Telework Rules of Behavior.

- NCA has inventoried, and will recall, all NCA-owned laptops to install the latest software updates including new VPN software, virus patches, and encryption software once it receives direction to do so.

- NCA will re-evaluate the need for external customers' access to our systems and strengthen controls for those customers who require access.

- NCA will develop a Policy Directive to require that new cemeteries implement individual Facility Security Handbooks prior to opening.

CONCLUSION

Our objective is to conduct day-to-day operations and accomplish our mission using security controls that are commensurate with risk, and to maintain a culture where our employees consistently and thoroughly safeguard VA data. NCA officials must assure that management, operational and technical safeguards are in place and are implemented to protect the confidentiality, integrity and availability of systems and data. They will do so. They must also assure that the systems and data are properly controlled and protected to prevent the real harms that can result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. They will do so. As Under Secretary for Memorial Affairs, I will see to that. I accept ultimate responsibility for assuring that these responsibilities are met throughout the National Cemetery Administration.

NCA people have always purposely pursued strategies necessary to safeguard information that is entrusted to them. They are dedicated to the mission of ensuring that the burial needs of veterans and eligible family members are met. Through continued review and diligence, they will ensure and I will ensure that the privacy of our veterans and their loved ones is preserved.

We welcome any guidance and assistance to improve NCA's security posture. We will continue to pursue best practices and we will work with you and

our VA colleagues to ensure that sensitive information entrusted to NCA custody is secure and safeguarded.

Thank you for the opportunity to appear before you today. I would be pleased to respond to any questions that you may have.

Statement for the Record of

Jonathan B. Perlin, MD, PhD, MSHA, FACP
Under Secretary for Health
Department of Veterans Affairs
before the
House Committee on Veterans' Affairs

June 29, 2006
***** *

Good morning, Mr. Chairman and Members of the Committee. Thank you for allowing me the opportunity to provide an overview of the security and privacy protections that Veterans Health Administration (VHA) has in place to protect the electronic health records and sensitive personal information of our veteran patients.

VHA is committed to providing the best possible health care to each of the 5.3 million patients we treat at our hospitals, clinics and other sites each year. Our nurses, doctors and other health care staff members devote themselves to delivering high-quality, compassionate care to these patients—the men and women who have bravely served our Nation. In VHA, as we carry out our mission, we are dedicated to fully protecting the security and privacy of veterans' medical information. It is one of our fundamental operational pillars.

Today, VA provides some of the best health care in the nation.[1] This is documented in the scientific literature and lay press. Patient satisfaction surveys say the same thing.[2] This outstanding level of patient care is due in large part to VistA – an Information Technology (IT) system that sets the gold standard for electronic health records.[3]

VistA is recognized as one of the best electronic health record systems in use anywhere. It is touted as a model for supporting the President's goal to implement electronic health records throughout the nation. At VA health care facilities around the country, it has helped doctors, nurses and other clinicians save tens of thousands of lives—and provide better, safer and more consistent care.

VHA has succeeded in integrating the electronic health record (including imaging and health-related bar code applications) in the day-to-day workflow of health care delivery processes to a greater degree than any other health care organization in the world.

VHA is responsible for protecting data on all systems that facilitate the delivery of healthcare benefits to our nation's veterans. Similar protections are provided for the

---

[1] Longman, P. (2005), 'The best care anywhere', *Washington Monthly,* 27 (January/February): 38-48.
[2] Asch, S.M., E.A. McGlynn and M.M. Hogan (2004), 'Comparison of quality of care, for patients in the Veterans Health Administration and patients in a national sample', *Annals of Internal Medicine*, 141: 938-945.
[3] Morgan, Matthew W. (2005), 'The VA Advantage: The Gold Standard in Clinical Informatics', *Healthcare Papers*, volume 5, no. 4, 26-29.

databases that contain the veteran health records exchanged between the Department of Defense (DoD) and VA. We protect many important health databases and systems that enable us to provide quality care to our veterans.

VHA systems contain considerable amounts of sensitive data that is used in the delivery of health care benefits to our veterans and their dependents. Sensitive data typically handled in VHA include, but are not limited to, medical/health and benefit data, personnel and employment data, individually identifiable data for veterans and employees, and financial data. VHA also handles various forms of storage media in support of systems operations.

Since VHA is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), VHA complies with the statutorily strict provisions of HIPAA through a comprehensive Privacy Program that provides oversight and guidance throughout VHA to ensure privacy of veterans' information is maintained. While the other VA Administrations and Staff Offices are not covered entities under HIPAA, they do comply with other Federal privacy laws, such as the Privacy Act of 1974.

VHA databases include:

- Veterans Health Information Systems and Technology Architecture (VISTA), the automated environment that gives VA clinicians near-real-time, secure access to the electronic health information available in the Computerized Patient Record System, or CPRS, and VistA Imaging.

  VistA is our core electronic health record system. This widely acclaimed system has saved the lives of thousands of veterans. But it was designed twenty years ago. As such, it is principally "hospital" based, and is deployed in more than 100 locations. This distributed nature does not lend itself to simple security compliance. Today, network and telecommunications standards and solutions exist to assist in mitigating these risks while creating greater efficiency and effectiveness. Later in my testimony, I will discuss the solutions we are developing to address these risks.

- My HealtheVet, a Web-based application that provides veterans, their families and clinicians secure access to trusted health information. My HealtheVet links to Federal and VA benefits and resources, the veteran's Personal Health Journal, and online VA prescription refill capability.

- The Federal Health Information Exchange/Bidirectional Health Information Exchange (FHIE/BHIE), a federal healthcare initiative that facilitates the secure, electronic exchange of patient medical information between government health organizations. FHIE/BHIE provides both VHA and DoD physicians access to health data at locations where patients receive care from both systems.

- The Health Data Repository (HDR), a repository of selected clinical data for every veteran who has received care in a VA hospital. Data from the HDR is used to create an historical, longitudinal picture of the veteran's health record, and is available to every clinician within the VA who provides care to a veteran. While the HDR database is not complete, we have populated it with clinical data in the areas of allergies, laboratory and out-patient pharmacy. We are continuing to add additional clinical data to the HDR database.
- The Clinical and Health Data Repository (CHDR) initiative, which seeks to ensure the interoperability of the DoD Clinical Data Repository with VA's HDR. CHDR permits the exchange of clinical data so that DoD Tricare and VA beneficiaries receive seamless care.

- VHA National Databases - VHA collects healthcare and administrative data in national databases, many of which are located in the secure environment of the VA Austin Automation Center. These data provide the foundation for understanding and improving the quality of VA healthcare, allocating resources across the organization, and managing operations.

All VHA systems in the VA's Federal Information Security Management Act (FISMA) inventory were certified and accredited and received authority to operate in 2005. A program to continuously monitor the effectiveness of the security controls in these systems, and to re-certify systems in accordance with VA policy is in place. All transmissions of data to and from My HealtheVet, CHDR, and FHIE/BHIE are encrypted to current Federal standards. VHA complies with all VA policies and develops additional health care-specific privacy and security policy and guidance.

The Rules of Behavior advise users that misuse of government systems, mishandling of veteran data, or unauthorized disclosure of sensitive information could result in disciplinary action up to and including termination of employment.

To protect VHA systems and data from unauthorized access, a number of security controls have been implemented. Let me address specific security procedures in place to control access, ensure continuity of operations and protect data.

Access
VHA carefully manages access to information system resources through a combination of technical and administrative controls. User access and verify codes are required to gain access to information system resources. Sensitive data can be accessed only by those with a legitimate and demonstrated need. Even then, users can access only the information needed to do their jobs. Granting access to users requires management approval, which is routed through the appropriate Information Security Officer (ISO). User access privileges are reviewed to ensure legitimate and continued need for access.

Storage
All VHA systems are backed up at least weekly in accordance with VA and VHA policy, or more often depending on the nature of the data. Several generations of backups are retained, and the restore process is tested regularly to ensure that data can be restored to its original state. The backups are stored at off-site locations, and appropriate physical and environmental controls are in place to protect the backups. Media used to record and store sensitive software or data are secured when not in use, or they are sanitized or destroyed in accordance with VA policy. Contingency plans are in place, and plans are "tested" as a consequence of system outages. VHA is focusing efforts on improving compliance with the requirement to document these tests.

Allow me to provide an example of how our backup procedures were employed after the New Orleans VA Medical Center was shut down and evacuated following Hurricane Katrina. Because telecommunications lines were down, back-up tapes of our electronic health records from the New Orleans facility were flown to Houston Veterans Affairs Medical Center and loaded onto systems. The VistA systems were back up and running in less than two days with no loss of data. This was a well-documented test that demonstrated effective backup procedures.

Security of Data in Transit
Data transmitted among VA systems are monitored 7 days a week, 24 hours a day, 365 days of the year, primarily for the purposes of system performance and availability. Data traffic moving inside the VA network (behind the firewall) is not encrypted; when VA data are sent outside the firewall, a Virtual Private Network, or VPN, is used. Data transiting the VPN tunnel are, by definition, encrypted. In addition, intrusion detection systems have been deployed; the VA Security Operations Center monitors these systems for the presence of unwanted intruders or attacks on VA networks. Data are encrypted in accordance with VA and VHA Directives 6210.

VPN Access
The VPN is a centralized service that provides secure, remote access to VA's employees and contractors. The OneVA-VPN grants remote access for individuals such as doctors, nurses and other clinicians who need access to data or information to perform their functions (e.g., patient care). Typically, these employees are logging into the system at home or during travel. Some off-site contractors also use VPN to access information essential to the performance of their tasks. Users must read, comprehend, sign, and abide by the Rules of Behavior form that requires signature before access is granted. Contractor access through the VPN is restricted to the locations appropriate to each contractor through Internet Protocol (IP) addresses. User access is authorized and controlled in accordance with VA remote access guidelines, and requires supervisory approval and confirmation with the supervisor by the appropriate ISO.

Contractor access must be approved by both the Contracting Officer Technical Representative and the ISO. Contractor accounts are established with VHA's business

partners who support remote maintenance for medical devices, provide medical transcription services or perform diagnostic radiology services.

Telework
The Department issues VPN user accounts and equipment for use by teleworkers at management's discretion. VPN user accounts, as described above, provide secure, remote access to VA systems and data. Telework agreements are signed by the employee and supervisor and describe the responsibilities and procedures for telework.

Telework is not open to everyone, nor to every type of work. The VA policy requires managers to determine whether it is appropriate for an employee to telework and whether it is appropriate for the work to be performed via a telework arrangement. If an authorized teleworker will be accessing sensitive documents, that person has received management approval and must agree to protect Government/VA records from unauthorized disclosure or damage in accordance with the requirements of the Privacy Act and all applicable Federal laws and regulations, VA Directive and Handbook 6210, and other applicable VA policies.

Security of Equipment Brought in to VA
All employees and contractors must follow VA policy when they bring in any non-VA computer equipment that is connected to the VA network. Before this equipment may be connected to the network, it must be scanned to ensure that it is in compliance with the latest operating system patches and virus updates. VHA will comply with any new guidance or directives issued regarding the use of non-VA computer equipment, as set forth by the Department.

Training Requirements
VHA follows VA policy regarding security and privacy training requirements. Employees and contractors must undergo initial security orientation before they can access VA systems. In addition, employees and contractors are mandated to complete annual security awareness training, which must be documented. Users must sign Rules of Behavior documents. Annual privacy training also is mandated. Privacy training must be completed within 30 days of an employee's or contractor's start date and before access to sensitive data can be granted. Both privacy and security training modules continue to be developed to target specific job responsibilities.

Enforcement of Procedures
Given the complexity of information technology systems, vulnerabilities will be discovered periodically. Therefore, on an ongoing basis, VHA performs internal risk assessments to identify our weaknesses. When our assessments identify vulnerabilities, we remediate the problems in the appropriate manner, including issuing new policy and making technical changes to the system.

Security and privacy policy compliance is monitored internally by annual FISMA security surveys, site security program reviews conducted by the VA Office of Cyber and Information Security and during VHA System-wide Ongoing Assessment and Review

Strategy (SOARS) site visits. SOARS visits are designed to review facility compliance with internal and external oversight groups {e.g., Office of Inspector General Combined Assessment Program (CAP) Reviews, Joint Commission on Accreditation of Healthcare Organizations (JCAHO)} standards prior to visits from these oversight groups. On an ongoing basis, the VHA Privacy Office conducts site assessments to ensure compliance with privacy policies and laws, and to provide direction on how to remediate problems. Additionally, VA's Office of Cyber and Information Security is currently letting a contract for independent validation and verification of VA's certification and accreditation documentation, testing, and approval-to-operate processes to ensure that VA certification and accreditation procedures comply with FISMA requirements.

VHA also has health-specific privacy programs enforced by Privacy Officers at each facility. Information security responsibilities are delineated in senior executives' performance plans. The effectiveness of the required security controls/policies are tested through the certification and accreditation process. Security and privacy violations are reported to a central entity, appropriately researched and resolved. Privacy violations are reported by the Privacy Officers to the Privacy Violation Tracking System, and security incidents are reported by the ISO to the VA Security Operations Center.

There are also external mechanisms promoting VHA compliance. Compliance with the Health Insurance Portability and Accountability Act (HIPAA), including the Privacy and Security Rules, is determined by the Department of Health and Human Services through its conduct of investigations in response to complaints or compliance reviews as appropriate. The Department of Justice monitors VHA Freedom of Information (FOIA) and Privacy Act compliance. The OIG monitors our compliance with all privacy and security requirements through CAP Reviews. Also, agencies such as JCAHO actively assess VA compliance with privacy and security requirements. Reviews of JCAHO findings in information management indicate that VA is doing well in this area.

Security and Privacy of DoD/VA Clinical Data Sharing

To illustrate the strength of our security and privacy measures, I would like to call your attention to the Department of Defense/VA electronic health data sharing program.

The Department of Veterans Affairs is the lead agent for FHIE/BHIE, the award-winning DoD/VA program that enables the two agencies to share the patient records of U.S. service members and veterans. Not only was FHIE/BHIE built to the highest standards, it also has received positive assessments from independent reviewers and high scores on National Institute of Standards and Technology criteria. It also is noteworthy to add that FHIE/BHIE was one of five winners of the prestigious Excellence.Gov award from the American Council for Technology for demonstrating best practices in information sharing for federally led IT program implementations.

To ensure the highest level of protection for the DoD and VA clinical data as it is sent across the Internet, the information is double-encrypted using DoD-approved software, effectively securing the transmission of all sensitive data from unauthorized access.

The data also traverses both Departments' firewalls via a hardware Virtual Private Network, which provides secure, remote access.

FHIE/BHIE is in full compliance with VA, DoD and Federal government information security policies and privacy rules. In December 2005, the system underwent recertification, and received renewal of its authority to operate decision.

VHA Actions In Response to OIG Vulnerabilities
In a recent report, the OIG identified 16 security vulnerabilities. VHA has taken a number of actions to address the nine unresolved security vulnerabilities within VHA's purview; the seven remaining actions are the responsibility of the Department. To verify that VHA has the appropriate safeguards in place for data security and privacy, VHA has taken the following actions: System-wide Ongoing Assessment and Review Strategy site visits, HIPAA/privacy site assessments, and a recent communication from the Deputy Under Secretary for Health for Operations and Management requiring local management to certify compliance with security safeguards consistent with OIG findings. VHA leadership has also been monitoring the completion of all deficiencies identified as a result of the completed certification and accreditation work. Related to the monitoring activities, a recent memo from the Principal Deputy Under Secretary for Health, reiterated the importance of security remediation and directed VHA system owners to complete all remaining actions by June 30, 2006.

The Deputy Under Secretary for Health for Operations and Management also issued a memorandum in May 2006 requiring all facilities to submit an inventory of external business partner gateways through their Veterans Integrated Services Network (VISN) offices; all VISNs have complied with this request. In addition, the facilities are required to prepare and submit the necessary paperwork for the gateways to the VA Enterprise Security Change Control Board for formal review and approval. VHA policy requires all older operating systems installed on medical equipment to be connected to facility networks using the VA's Isolation Architecture as published in April 2004. This architecture provides increased security controls through a well-defined structure of isolation from the facility's main information network.

VHA's change control procedures are in the process of being addressed through several actions, which involves the strengthening of the current software development governance process. VHA is instituting a rigorous Capability Maturity Model Integration approach with assistance from Carnegie Mellon's Software Engineering Institute. The outcome of the approach is a fully integrated and effective configuration management and change control process implemented across the organization.

VHA has implemented security controls to address wireless security vulnerabilities, but recognizes that there are a number of policies, procedures and tools that need to be implemented to improve VHA's ability to protect IT systems and data in the wireless environment. A workgroup has been formed to address wireless requirements from an organizational perspective to comply with OIG vulnerability assessments and recommendations. The workgroup is charged with developing a wireless security

controls test plan for facilities, identifying standard tools to improve management and control of the wireless environment, and developing associated policy templates and assessment checklists.

Privacy/Security Issue

Since the unfortunate theft occurred of veteran data, while it did not include VHA health care data, VHA has used this as an opportunity to validate its ongoing security and privacy practices, has re-educated its employees and contractors about privacy and security, and has begun making bold changes where necessary. These decisive actions are in addition to the many other measures VHA takes on an ongoing basis to ensure the security and privacy of our veterans' medical information.

A privacy and security issue was brought to light in 2005 when a sub-contractor in India threatened to expose medical records of veterans due to non-payment by their contractor.[4] VA had originally provided the medical information to a transcription company, and was alarmed to learn that VA-contracted medical transcription services had been subcontracted to an offshore company without our knowledge. Various offices within VA, including the OIG, the Office of the General Counsel, and VHA were involved in the review, investigation and resolution of this matter. Though VHA determined that no privacy disclosure violation had occurred in this incident under the Privacy Act of 1974 or Health Insurance Portability and Accountability Act (HIPAA), action was taken to ensure that no VHA programs were contracting for non-domestic transcription services. A settlement agreement reached in this matter included an agreement to destroy all records that the vendor had in its possession. A certification was subsequently received from the vendor stating that it had permanently destroyed all hard copies of records and deleted all electronic files containing VA medical records.

In response to the concerns raised by this incident and concerns regarding contractors using offshore or non-domestic subcontractors, VHA issued a moratorium on contracting for non-domestic telehealth services in May 2005. In addition, the Business Associate Agreement (BAA) template was revised to include language requiring contractors to only use subcontractors or agents who are physically located within a jurisdiction subject to the laws of the United States. The Under Secretary for Health further strengthened VHA's position to prohibit offshore work in a memorandum issued in June 2006 that permanently requires contractors to transcribe in the United States or its territories, and requires all facilities to have BAAs in place. Transcription vendors contracted by VHA must also sign BAAs in addition to following Privacy Act requirements.

We also are developing recommendations for a uniform approach to transcription and speech recognition to be used throughout VHA. VA is now gathering information on current contracts and experience with speech recognition technologies. The VHA Clinical Logistics Office will coordinate an interdisciplinary workgroup to review this data and prepare a report with recommendations on the feasibility of a national contract for

[4] OIG Draft Report, Audit of the Veterans Health Administration's Acquisition of Medical Transcription Services, Project Number 2004-00018-R3-0195

transcription services, a national roll-out of speech recognition technologies, or a combination of the two in VHA, along with cost information. The report and recommendations are due in October, 2006, with implementation to follow.

Actions to Further Strengthen Security and Privacy
At VHA, the security and privacy of veteran information is of paramount concern, and VA and VHA are committed to continuing to strengthen our security and privacy controls. To this end, VA is investigating the use of encryption solutions appropriate for our information systems and data protection needs. VHA is also re-engineering current applications to broaden auditing capabilities, and continue to implement enhancements to its existing role-based access mechanisms to ensure that access to information is based on defined roles.

The next generation of VistA, which is being developed now, will have enhanced security controls built into the system. This widely acclaimed system has saved the lives of tens of thousands of veterans. But it was designed twenty years ago. As such, it is principally "hospital" based, and is deployed in more than 100 locations. This distributed nature does not lend itself to simple security compliance. Today, network and telecommunications standards and solutions exist to assist in mitigating these risks while creating greater efficiency and effectiveness. In the next generation of VistA, role-based access control permissions will be much more granular than the access controls in VistA today, enabling tighter management of user permissions across all applications as well as the ability to set system operations (e.g., create, read, update, delete, execute) for data and software applications. These enhanced processes will be employed to address need to know, least privilege, and separation of duty principles. Many other technical and procedural security controls are also being identified in VHA's security requirements repository for implementation across the system development life cycle for the next generation of VistA.

VHA already has strong security procedures in place, yet these procedures can be strengthened. We can do this by enhancing privacy and security guidance, through strong directives with enforceable actions, by conducting regular privacy and security-awareness training led by senior VHA leadership, and by emphasizing privacy and security education.

The recent theft of data that occurred has emphasized the need for extra vigilance in the use of the data that enables us to carryout our mission. The Secretary is developing a plan for VA to become the Gold Standard in the areas of security and privacy. VHA actively supports this direction.

House Veterans Affairs Committee
June 29, 2006

Hon. Gordon H. Mansfield
Deputy Secretary of Veterans Affairs

Mr. Chairman and Members of the Committee. Thank you for this opportunity to appear before the House Committee on Veterans Affairs.

The Secretary has acted decisively to determine the scope of the loss of data, ascertain its impact and act affirmatively to address what we must do to protect our veterans. He has directed changes that will affect the culture of this department and has moved information security to the forefront of our consciousness.

This loss was tragic on many levels, but it is important to note that the data that was stolen was a copy of other data that is still in VA's possession i.e. it was not a loss to the VA.

As has been noted in previous hearings, it is useful to discuss our efforts in a few basic parts: (1) what we have done; (2) what we are doing; (3) what needs to be done; and (4) how we will measure our progress. The Secretary has stressed to senior staff that, our goal, is to have the VA be the *Gold Standard* in the realm of cyber and information security, just as it has become in the realm of electronic medical records and the delivery of healthcare to veterans.

What we have done
Following the theft of data from a VA employee's home, we retained forensic experts to determine the extent of potential loss. Once the magnitude of the loss was more fully understood, we have been working non-stop to take steps as appropriate – going forward – to protect our veterans.

As previously announced, the Secretary has:

Implemented a series of personnel changes in the Office of Policy and Planning, where the breach occurred. Recently-retired Admiral Patrick Dunne has been nominated by the President to be Assistant Secretary for Policy and Planning. With his confirmation, he will bring the much needed leadership to that office. Admiral Dunne is working now at VA as a consultant.

Has retained Richard Romley as an outside, independent advisor to the Secretary. He has significant experience in data theft, governmental reorganization and critical issue development. As a former prosecutor, Rick has a reputation for independence and a unique ability to get to the bottom of issues.

Has expedited completion of Cyber Security Awareness Training and Privacy Awareness Training for all VA employees. He has directed that all employees have this training prior to the end of June.

He has directed that VA facilities across the country – every hospital, Community-Based Outpatient Clinic (CBOC), regional office, national cemetery, field office and VA's Central Office – observe Security Awareness Week which began Monday, June 26th. Throughout this week, each office will focus on different aspects of cyber and information security, how those pertain to their particular operation, and how to assure that security is an integral part of the work place ethic.

- VA's initial response to the data loss was to mail over 17.5 million letters advising individuals of this data loss, and providing them with a toll free number which will outline proactive steps they can take to protect themselves. This call center immediately provided the capacity to handle up to an additional 260,000 calls a day. The volume of calls has been less than we expected.

What we are doing – Specific Actions

At a recent press conference, the Secretary announced that VA would be providing free credit monitoring to all affected veterans who sought that service. That service will also include an insurance component to help minimize any personal out of pocket expenses, should a veteran's identity be compromised as a result of this loss. We were preparing to issue a request for proposals to vendors capable of providing this service. Last Friday, the Federal District Court in Kentucky hearing one of the class action lawsuits emanating from this data theft, issued a Temporary Restraining Order barring the government from publicizing its free credit monitoring offer to veterans whose personal data was stolen.

The Secretary has also directed that every laptop computer in VA undergo a security review to ensure that all security and virus software is current, including the immediate removal of any unauthorized information or software and the application of appropriate encryption programs. But, because of the pending lawsuits, this directive has been placed on hold until we obtain guidance from the courts.

In addition, we have been in discussions with corporations which provide unique data breach analysis to see if data is being exploited and we anticipate entering into a contract shortly for this service.

We are making an effort to be responsive to concerns, expressed at a recent hearing, that we provide "detection, protection and insurance," essentially a credit protection and resolution package, for those possibly affected. It is appropriate that we do this.

The Secretary has directed that VA conduct an inventory of all positions requiring access to sensitive VA data by August 31, 2006, to ensure that only those employees who need such access to do their jobs have it. And we will be developing the procedures

necessary to assure that employees have an appropriate level of background check in place, and that those be updated on a regular basis. For example, the employee from whom data was stolen had not had a background investigation for 32 years.

As the chief operating officer of the Department;

- I have overseen issuance of IT Directive 06-1, *Data Security-Assessment and Strengthening of Controls* on May 24, 2006. This directs all three VA administrations and staff offices to review existing internal methods of storing, transmitting and protecting sensitive data. It also calls for a review of current procedures and VA-wide actions to date through a series of briefings attended by key departmental officials during the months of May and June.
  I have reviewed Directive 07-10. This is as system of determining what time of background check and information access is necessary per occupation title.
  I have overseen the issuance of VA Directive 6504 on June 12, 2006. This directive provided policy regarding transmission, transportation and use of, and access to, VA data outside VA facilities.
  Along with internal actions, I communicated the Department's actions with various Members of Congress and their staffs-to include coming here to discuss matters with committee staff.

What we are doing – Major IT Reorganization within VA

In October 2005 the Secretary issued a directive to implement the reorganization of IT within VA. Pursuant to that reorganization, more than 4,610 IT professionals engaged in operations and maintenance of the Department's IT infrastructure, plus 560 unencumbered positions, have been detailed to the Office of Information and Technology, under the direction of the Chief Information Officer. As of the beginning of the new Fiscal Year on October 1, 2006, those details will become permanent, thereby establishing a new career field within OIT.

In this IT reorganization, all IT professionals are being consolidated into the Office of Information and Technology, except for certain Development Domain personnel in VHA and VBA. These developers will also be brought under the control of the CIO as well.

They will look to the CIO for:

1. Budget Direction/ and OMB exhibit 300
2. Security Requirements
3. System Standards; and
4. Enterprise Architecture Requirements

Other major milestones include the establishment of the position of Chief Financial Officer with budget authority in the Office of Information and Technology. This new office is being established to give the CIO control over all Departmental IT funds.

Security has been centralized under the CIO. All Department Information Security Officers (ISOs) have been detailed to the CIO

This situation has highlighted for us the fact that we have not had the right policies, procedures, guidelines, regulations and directives in place – with the teeth to enforce them – to assure that those nominally responsible for security could effectively do their job. This is why the Department has acted aggressively in implementing stronger administrative procedures.

For example, the IT operation today has evolved over time and has included the services of many talented and dedicated professionals. Their efforts are paying off. For example, in terms of cyber security, VA IT systems are:

1. Certified
2. Accredited, and
3. External independent gateways have been reduced.

We will continue to implement IG recommendations as warranted.

What we are doing – IT Assessment

The range of IT programs administered by the Department on behalf of our veteran clientele is extensive. As a result, the array of hardware and software, where it is located, the number of systems, the number of persons having access to data, how that access is granted or denied, how the data is utilized and by whom, what background checks are needed – all have grown tremendously over the years. These are areas that require out immediate review, and, where necessary, remediation.

This theft of VA data has been a wake up call to all of us—at VA and in government in general. IG reports in the past years have highlighted specific weaknesses, but as an institution, VA did not respond to those with the sense of urgency that, in retrospect, was called for. With benefit of hindsight, that need for urgency is overwhelmingly apparent today. We recognize that we must change the culture of the Department, and we have embarked on doing just that.

We have also directed that previously authorized work procedures which allowed employees to transport hard copies of claims folders to alternative work sites be stopped. It is a government-wide practice to encourage telework or telecommuting, especially in the Washington metropolitan area. Yet we must assure that our policies and procedures implementing this are such that sensitive data relating to our veterans is properly protected. Our Acting Undersecretary for Benefits is to review and revise his own guidance to his staff in this area to ensure the protection of veterans' vital records and sensitive data prior to resuming this practice, if at all.

What we are doing – Regulations and Guidelines

We are working to assure that we have clear guidance for all VA employees in place, and that they are aware of what is required of them – and of the consequences, should they fail to adhere to that guidance, which sets forth the guidelines for information security and the enforcement mechanisms pertaining to that. This document is designed to eliminate any confusion as to what is expected of Departmental employees concerning security of data.

Measurement of Success

How will we measure our success in this endeavor?

One measure of success is to correct deficiencies noted by the IG in the past.

Additionally, we will improve our FISMA compliance. As I noted, in the past we received an "F" on the FISMA scorecard. That is unacceptable, and we must do better in the future.

And we will continue to communicate with VA employees that which is expected of them to comply with information and data security.

What needs to be done – Legislation

The Health Insurance Portability and Accountability Act (HIPAA) governs all aspects of the privacy of sensitive information pertaining to an individual's health. HIPAA provides for criminal penalties of up to 20 years imprisonment and a fine of up to $250,000 for intentional misuse of health information for private gain.

There is no comparable law pertaining to the misuse of other non-health, sensitive, personal information, and I echo the Secretary's call that the Congress should enact such a law. Someone intent on fraudulently using personal information may think twice if he or she focuses on severe penalties that could be encountered for such a crime.

Conclusion

Mr. Chairman, the fixes we have outlined won't be easy, and it won't be overnight, but I am absolutely convinced that we can do it. We have as goal to become the "Gold standard" just as it has become the 'model' for health care in the United States.

Mr. Chairman, that concludes my testimony.

###

Statement of Ronald R. Aument
Deputy Under Secretary for Benefits
Before the
House Committee on Veterans Affairs
June 29, 2006

Mr. Chairman and Members of the Committee, thank you for the opportunity to provide testimony on data security in the Veterans Benefits Administration (VBA).

As a result of the most unfortunate theft of data from the home of a VA employee, VBA is conducting a thorough examination of every aspect of our information security program, our processes, and our procedures to ensure that sensitive veterans' data is neither mismanaged nor used for any unauthorized purpose. This statement outlines the security measures VBA had in place prior to May 3, 2006, what we have done to communicate with veterans about the data theft, and additional steps we have taken regarding our data security policies and procedures. It also specifically addresses the security of the data feeds between VBA and DoD.

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

IT SECURITY POLICIES AND INITIATIVES PRIOR TO MAY 3, 2006

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

as well as to those individuals, including consultants, to whom VBA authorizes access to VBA systems and data.

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

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

Under the IT reorganization, VBA business lines retain an important support role in the internal management of IT security. VBA continues to be responsible for managing data, its use and disposition. We fully understand the importance of securing access to our systems as required by the FISMA and Certification and Accreditation (C&A) processes. VBA business lines are responsible for authorizing access to VBA computer applications at the appropriate security levels. True business "need to know" must be established, and compliance with the various legal requirements of the Privacy Act, Freedom of Information Act, Privacy Act Systems of Records, and memorandums of agreement must be determined before access is authorized.

The standard configuration of VBA servers and desktop and laptop computers is centrally controlled. Updates are deployed automatically to maintain quality assurance and security. When a server or workstation is connected to the network, the VBA standard configuration is automatically loaded.

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

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

VBA has established rules-of-behavior policies that comply with VA requirements and govern the use of IT systems and capabilities maintained by or for VA. All users authorized to access VA systems through Local Area Networks or through the One VA Virtual Private Network are required to sign VBA-specific rules of behavior. VBA rules of behavior have also been developed for

employees authorized to use government-owned laptop computers. These VBA rules of behavior ensure all users of VA IT resources are aware that any system potentially contains valuable and sometimes sensitive government and/or personal information, which must be protected to prevent disclosure, unauthorized changes, and loss.

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

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

VBA also has a formal process for requesting data extracts from VBA information systems. A Project Initiation Request (PIR) is a request to the VBA Office of Information Management (OIM) for information technology services initiated by both VBA and VA entities. The PIR is prepared primarily by a sponsor organization to notify OIM of a new system requirement, a modification or change to a requirement, an enhancement to an existing system, or a request

for a data extract or match. For example, VBA provides 15 different extracts from the Beneficiary Identification and Records Locator System (BIRLS) to internal VA organizational elements as well as external agencies. Data is matched and/or extracted from BIRLS for purposes such as identification of inactive claims folders eligible for retirement to a storage facility; verification of veteran status for Department of Education benefit applicants; identification of VA employees in the PAID system who are also veterans; death matches with the Veterans Health Administration and the Social Security Administration; investigations by the Office of the Inspector General; and research projects by the National Academy of Sciences Institute of Medicine. Additionally, there are four interfaces or data feeds into BIRLS: two from the Defense Manpower Data Center for new servicemembers and reservists and to provide retired pay information; one from the VBA Benefits Delivery Network (BDN) claims processing system to update BIRLS based on recent BDN record changes and transactions; and one from the Veterans Assistance Discharge System (VADS) for recent separatees. Each extract and interface was established through a formal VBA approval process. Modification of any data provided electronically is prohibited.

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

VBA Network Support Centers also conduct annual surveys of IT operations and security controls, policies, and procedures at their client ROs within their geographical area of jurisdiction. The primary purpose of these on-site security visits is to ensure that the ROs are adhering to all VA, VBA, and

other federal security directives and handbooks and that deficiencies identified in previous CAP reviews are remediated.

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

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

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

As part of our ongoing efforts to strengthen IT security, VBA has successfully tested its disaster recovery procedures for 29 of 31 major

applications, and has invested in a fully redundant system to provide disaster recovery for the Benefits Delivery Network (BDN). The system has been installed, and a test of the recovery of all BDN applications was completed in September 2005. The test will be repeated yearly.

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

Specific Business Line Access Issues

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

Veterans Service Organization (VSO) Access to Veterans' Information

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

VSO representatives who are co-located at VBA sites, as well as many VSO representatives who work at non-VA facilities, have access to some of the same IT systems which VA employees access. These systems are restricted so that VSO representatives can only access information regarding their organization's clients, and only if they have a power of attorney. In addition to VA's procedures for safeguarding sensitive information, the Veterans Service Organizations themselves have procedures for controlling access and dissemination of such information. The One-VA Virtual Private Network (VPN) allows remote VSO users to access VA systems in a secure environment.

Outbased Employees

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

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

QTC Medical Examinations

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

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

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

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

Vocational Rehabilitation and Employment Contract Counselors

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

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

Loan Guaranty Contractors

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

ACTIONS TAKEN TO INFORM VETERANS ABOUT THE DATA THEFT

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

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

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

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

TECHNICAL AND POLICY CHANGES SINCE DATA LOSS INCIDENT

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

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

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

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

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

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

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

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

DoD DATA FEEDS

The VA/DoD Joint Executive Council (JEC) was established as a result of the President's Management Agenda. This council is charged with enhancing coordination and resource sharing between VA and DoD and satisfying the reporting requirements of Public Law 97-174 and Public Law 108-136. VA and DoD together have made substantial progress toward data sharing strategies

essential to demographic data exchange and data synchronization. Additionally, we continue to make progress toward simplifying registration and enrollment of veterans, as well as the way we manage contact with veterans throughout their lifetime.

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

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

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

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

June 28, 2006

Commemorating 75 Years of Service

The Honorable Steve Buyer
Chairman
Committee on Veterans' Affairs
U. S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am sending to you the Memorandum I issued today which delegated to the Assistant Secretary for Information Technology (IT) full authority, responsibility, and enforcement for departmental information security. This is the matter that I mentioned yesterday.

I am confident that this delegation will assist greatly by clearly empowering the CIO with both authority and responsibility. It should have been done years ago.

I would like to thank you for your time and consideration.

Sincerely yours,

R. James Nicholson

Enclosure

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

June 28, 2006

Commemorating 75 Years of Service

MEMORANDUM FOR THE ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY

SUBJECT: Delegation of Authority for Responsibility for Departmental Information Security

1. PURPOSE OF DELEGATION: The security of the Department of Veterans Affairs' (VA) information is the individual and collective responsibility of all VA personnel, contractors, volunteers, business partners, and other authorized users. Under the provisions of the Federal Information Security Management Act, the Assistant Secretary for Information Technology (IT) is required to establish and maintain the VA Information Security Program. This program involves the establishment of policies, procedures, practices, and requirements; the provision of oversight; and direction to implement the elements of the Information Security Program to all VA personnel. Additionally, the Assistant Secretary for IT is responsible for all facets of VA's information security, including budgeting for minimum mandatory security controls, training and awareness, certification and accreditation of VA's IT systems, incident response, and security systems engineering. As part of the continuing implementation of the Department's information technology realignment and our transition to the Department's seamless IT management structure, I am issuing this delegation.

2. DELEGATION. This memorandum delegates to the Assistant Secretary for IT complete responsibility and complete authority for enforcement of information security policies, procedures, and practices. This includes, but is not limited to, the authority to:

- Establish standards for access to VA information systems by organizations and individual employees, and to deny access as appropriate;
- Order Department-wide compliance with and execution of any information-security policy;
- Direct that any incidents of failure to comply with established information-security policies be immediately reported to the Chief Information Officer (CIO);
- Report any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official for appropriate disciplinary action;
- Report any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official along with taking the appropriate corrective action; and
- Require any key official who is so notified to report back to the CIO regarding what action is to be taken in response to any compliance failure or policy violation reported by the CIO.

This delegation of authority also extends to those areas of responsibility that are related to information security, and are currently under the management and oversight of other Departmental organizations. For example, the Assistant Secretary for IT is herein delegated any authorities necessary to bring the policies, procedures, and practices relating to such activities as background investigations on employees and contractors and determination of risk and sensitivity levels of employee position descriptions into compliance with information security statute and regulation. This authority includes the Assistant Secretary for IT's approval of all associated polices and procedures, as well as the authority and responsibility for auditing of, and inspection related to compliance with, information security aspects of those approved directives. Further, this authority includes responsibility for issuing policies and procedures for the physical security of information, including responsibility for information security policies and procedures related to information security in offices, computer spaces, and buildings.

3. AUTHORITIES DELEGATED: The responsibilities of the Secretary under the Federal Information Security Management Act, 44 USC 3544; and the information security aspects of the following authorities: 5 CFR Parts 731 and 732; Executive Orders 10450, 12958, and 12968; and VA Directive and Handbook 0710 and authorities cited in that Directive.

4. RESTRICTIONS. None. This delegation cancels and supersedes all previous delegations of these authorities in the Department.

5. REDELEGATION. The Assistant Secretary for IT may further redelegate this delegation.

6. EFFECTIVE DATE. This delegation of authority is effective upon signature.

R. James Nicholson

EMPLOYEE HOME USE AMENDMENT
TO VA LICENSE AGREEMENT

Employee name and address: A

_____ ("Employee")

Customer currently licenses software ("Software") associated with the above-referenced Site under a Federal Supply Schedule Contract ("Agreement"). By signing below, , and Customer agree to modify the terms under which the Software is licensed for that Site as follows:

"Notwithstanding any language in the Agreement to the contrary, Customer's employees may use workstation or personal computer Software at home subject to the following terms:

1. the employee's use of the Software is governed by the Agreement;
2. the Software source code is a trade secret of the which the employee is not authorized to access, therefore, the employee will not modify, reverse assemble, reverse engineer, decompile or otherwise attempt to recreate the Software source code;
3. the employee will not copy or permit copying or access to the Software by any third party;
4. the employee will use the Software for Customer's work-related projects only;
5. the employee shall return the Software to Customer and destroy any copies of the Software if no longer an employee of Customer or if Customer discontinues the Software license;
6. Customer shall: (a) keep records of where the Software is being used; (b) if user based licensing applies, keep records of how many users are accessing the Software; and (c) provide the above information to the Institute upon request; and
7. Customer is responsible for any violations of these terms by the Customer's employees.

For Software licensed by total number of users, one employee using the Software both at work and at home shall be counted as one (1) user. For Software licensed by the number of workstations or copies, one employee using the Software on an employee workstation at home and on a Customer workstation at work shall be counted as utilizing two (2) copies. Customer shall ensure that the total number of workstations on which the Software is installed does not exceed the total number of copies licensed under the Agreement."

Except as herein modified, all terms and conditions of the Agreement shall remain in full force and effect.

Accepted by:

Employee:

By

Name

Info. Technology Specialist
Title

On Sept. 5, 2002
Date

By

Name (type or print)

Programmer
Title

On 9-5-02
Date

lg01.0013/6499 200.40.8010

OPTIONAL FORM 7 SEPTEMBER 1968 PRESCRIBED BY GSA FPMR (41 CFR) 101-20.110	**PROPERTY PASS**	1. DATE ISSUED

This pass is to be used whenever property is removed from the building. It is to be properly filled in and signed and handed to the guard when leaving the building.

2. NAME	3. BUILDING 810 Vermont ave.

4. DESCRIPTION OF PROPERTY BEING REMOVED

Laptop Computer and accessories
Barcode# 101 323816

5. PROPERTY BELONGS TO	6. DEPARTMENT OR AGENCY
Policy, Planning & Preparid	Dept. of Veterans Affairs
7. SIGNATURE OF PERSON AUTHORIZING REMOVAL OF PROPERTY ------ --------	8. TITLE 9. PASS GOOD UNTIL

JetForm

Justification for Access to SSNs

The Policy Analysis Service (008A1) conducts OMB approved National Survey of Veterans to collect data to be used for policy analyses and planning purposes. Administrative files such as the C&P files and medical files are often used as partial sampling frames supplemented with a Random Digit Dialing telephone methodology. Veterans not selected from VA administrative files are asked their real SSN in order that these may be matched against the administrative lists to determine if these veterans had more than one chance to be selected. These real SSNs are also used for matching purposes to supplement data requested on the survey in order to reduce respondent burden. These data are protected under the Privacy Act and a System of Records exists for the surveys and matched information. is the lead programmer within the Policy Analysis Service and as such needs access to real SSNs.

er

Office of the Assistant Secretary
For Policy and Planning
2/5/02

Done
2/5/02